TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

# ASIAKASJÄRJESTELMIEN TURVAAMINEN HYÖKKÄYKSENESTOJÄRJESTELMÄLLÄ

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-neuvoston kokouksessa 6. huhti-kuussa 2016

# TIIVISTELMÄ

**TERO JÄRVENPÄÄ**: Asiakasjärjestelmien turvaaminen hyökkäyksenestojärjestelmällä
Tampereen teknillinen yliopisto
Diplomityö, 54 sivua, 3 liitesivua
Toukokuu 2016
Signaalinkäsittelyn ja tietoliikennetekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Communication Systems and Networks
Tarkastaja: professori Jarmo Harju

Avainsanat: hyökkäyksenestojärjestelmä, verkon tietoturva, tuotteistus, palomuuri

Verkkohyökkäysten määrän alati kasvaessa pelkkä palomuuri ei enää nykyään riitä palveluiden kattavaan suojaukseen. Tällaisiin tilanteisiin ratkaisuksi sopivat erilaiset hyökkäyksenestojärjestelmät. Omassa ylläpidossa olevien palveluiden suojaaminen on helposti ratkaistavissa hankkimalla hyökkäyksenestolaitteisto tai -palvelu sopivalta toimittajalta. Mikäli käyttöpalveluita ostetaan kuitenkin yritykseltä, joka myös hoitaa verkkopalveluiden ylläpidon, luontevin hyökkäyksenestopalvelun tarjoaja on sama yritys. Tällainen hyökkäyksenestopalvelu voidaan toteuttaa monella eri tavalla, joista yhtä käsitellään tämän työn puitteissa

Hyökkäyksenestopalvelun tarjoamisessa suurin kuluerä on todennäköisimmin palvelusta aiheutuvat ylläpitokustannukset, joten keskeisenä suunnittelun lähtökohtana tuli olla niiden minimointi. Suorituskyvyllisesti palvelun toteuttava laitteisto tuli mitoittaa arvioidun asiakasliikenteen määrän mukaan. Asiakasjärjestelmiä suojattaessa myös järjestelmän valvontamahdollisuudet ja erilaiset rajapinnat muihin järjestelmiin nousevat suurempaan arvoon.

Hyökkäyksenestopalvelu toteutettiin Ciscon IPS-järjestelmän päälle. Järjestelmä hankittiin palomuurien yhteydessä toimivina sovellusmoduuleina, joten ylimääräisiä laitehankintoja ei tarvinnut tehdä. Moduulien käyttöönottoon ja konfigurointiin laadittiin suunnitelmat, jotta se ei häirinnyt palomuurien toimintaa. Järjestelmän toiminta pyrittiin samaan mahdollisimman automaattiseksi, ja ilmoitustoiminnallisuudet konfiguroimaan siten, että ilmoitus tulee oikeasti vain tilanteista, jotka edellyttävät muuta reagointia. Lokin kerääminen toteutettiin ulkoisen järjestelmän avulla, jotta tarvittaessa voidaan tarkemmin selvittää ja raportoida IPS:n tekemiä toimenpiteitä.

Tuotteen jatkuvuuden näkökulmasta on tärkeää, että se ei nojaa liikaa mihinkään sen toteutukseen käytettyyn teknologiaan, jotta tuotteen elinkaari voi jatkua teknologian elinkaaren päätyttyä ilman että asiakkaille suunnattu tarjooma merkittävästi muuttuu.

# ABSTRACT

**TERO JÄRVENPÄÄ**: Securing customer services using intrusion prevention system
Tampere University of Technology
Master of Science Thesis, 54 pages, 3 Appendix pages
May 2016
Master's Degree Programme in Signal Processing and Communications
Major: Communication Networks and Protocols
Examiner: Professor Jarmo Harju

Keywords: intrusion prevention system, network security, productisation, firewall

As the amount of network attacks keeps rising, basic firewall is no longer enough to offer required amount of protection for network services. Intrusion prevention systems are one way to alleviate the situation. Acquiring an IPS device or a service is a straightforward way to protect networks. However, if another company is hosting the services then the same company should also be able to offer some kind of an IPS service. There are many ways how this kind of a service can be implemented and one of these ways is presented in this thesis.

The greatestindividual expense in offering an IPS service is most likely the maintenance cost caused by the service. Therefore one of the most important things to reconsider in designing the service is to minimize the administration work as much as possible. The amount of processing performance required of the device should be measured according to the approximated amount of traffic generated by the potential customers. Also different kinds of monitoring capabilities and interfaces to other systems are even more important when securing customer systems.

The IPS service implemented within the scope of this thesis is based on Cisco intrusion prevention system. The system was acquired as a software module that can be installed on the physical firewalls. This way no additional deviceswere required. Installing and configuring the module was planned carefully so that no interference would be caused to the firewall. The day-to-day operation of the system was automated as much as possible and configured to notify the administrators only when additional actions were required. However, collecting the logs at all times is important so that actions taken by the IPS can analysed further if needed.

All in all, the IPS service created meets the requirements set for it. It is important to note that the created service cannot depend too much upon any specific attribute of the IPS technology it is based upon. This way the service can outlive the technology and a newer IPS technology can be used to replace the older one.

# ALKUSANAT

Diplomityö oli se viimeinen haaste valmistumisen tiellä ja nyt muutaman vuoden odotuksen jälkeen järjestyi riittävästi aikaa työn tekemiseen. Työ tehtiin Ambientia Oy:lle, jossa olen työskennellyt viimeiset viisi vuotta.

Kiitokset aiheesta ja työnohjauksesta esimiehelleni Matias Mäkiselle. Haluan myös kiittää professori Jarmo Harjua saamastani palautteesta ja ohjauksesta kirjoitustyön aikana. Kiitos myös Päiville pilkkusääntöjen kertaamisesta ja aikataulujeni sietämisestä. Erityiskiitos myös vanhemmilleni, jotka ovat vuosien ajan jaksaneet muistuttaa valmistumisen tärkeydestä.

Pirkkalassa, 24.5.2016

Tero Järvenpää

# SISÄLLYSLUETTELO

# LYHENTEET JA MERKINNÄT

| | |
|---|---|
| CDN | Content Delivery Network. Hajautettu sisällönjakeluverkko. Yleensä ympäri maailmaa sijaitsevien välimuistipalvelinten muodostama verkko, jonka avulla samaa sisältöä voidaan tarjota ympäri maailmaa mahdollisimman tehokkaasti. |
| CSV | Comma Separated Values. Tiedostomuoto, jolla voidaan esittää taulukkomuotoista dataa yksinkertaisessa tekstitiedostossa. |
| DOS | Denial of Service. Palvelunestohyökkäys. Hyökkäys, jolla pyritään estämään kohdepalvelun normaali käyttö. |
| ICMP | Internet Control Message Protocol. Nopeiden viestien lähetykseen tarkoitettu kontrolliprotokolla. |
| IDPS | Termi, jolla viitataan sekä IDS- että IPS-järjestelmiin |
| IDS | Intrusion Detection System. Hyökkäyksenhavainnointijärjestelmä. Järjestelmä, joka pystyy tunnistamaan kohdepalveluihin kohdistettuja verkkohyökkäyksiä tai muuta haittaliikennettä. |
| IoT | Internet of Things. Esineiden Internet. Internetin leviäminen esineisiin ja koneisiin, jotta esim. niiden tilaa voidaan valvoa etäältä. |
| IPS | Intrusion Prevention System. Hyökkäyksenestojärjestelmä. Kuin IDS-järjestelmä, mutta pystyy havainnoinnin lisäksi tarvittaessa estämään haittaliikennettä. |
| Liferay | Java-pohjainen alusta verkkopalveluiden toteutukseen. |
| Magento | PHP-pohjainen alusta verkkokauppojen toteutukseen. |
| NGFW | Next Generation Firewall. Uuden sukupolven palomuuri. Palomuuri, joka pystyy suodattamaan liikennettä myös OSI-mallin ylempien kerroksien datan perusteella. |
| NTP | Network Time Protocol. Ajan synkronointiin tarkoitettu protokolla. |
| OSI-malli | Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien kerrostumisen ja toiminnan kuvaamiseen käytetty malli. |
| PCI-DSS | Payment Card Industry Data Security Standard. Maksukorttijärjestöjen kehittämä tietoturvastandardi korttimaksamisen turvaamiseen. |
| Ping of Death | Verkkohyökkäys, joka perustuu Ping-toiminnallisuuden väärinkäyttöön. |
| RFC | Request for Comments. Internet-standardien julkaisuun käytetty dokumentti. |
| SDEE | Security Device Event Exchange. Standardi, joka määrittelee muodon ja protokolla, joilla laitteet vaihtavat turvallisuuteen liittyvää tapahtumatietoa. |
| Slowloris | Palvelunestohyökkäys, joka pyrkii avaamaan mahdollisimman paljon yhteyksiä kohdepalvelimelle hitaasti, ja pitämään niitä auki mahdollisimman kauan. |
| SNMP | Simple Network Management Protocol. Protokolla, jota käytetään laitteiden tilan raportointiin ja valvontaan. |
| SNMP TRAP | Tietynlainen SNMP-viesti, jolla SNMP-agentti voi ilmoittaa tapahtumista valvontajärjestelmälle. |
| SQL | Structured Query language. Kyselykieli, jolla relaatiotietokantoihin voidaan tehdä erilaisia operaatioita. |

| | |
|---|---|
| SSL | Secure Sockets Layer. Salausprotokolla, jolla voidaan suojata esimerkiksi Internet-sovellusten välistä liikennettä. Toiminta perustuu sertifikaatteihin. |
| Syslog | Lokitietojen välitykseen luotu standardi. |
| TCP | Transmission Control Protocol. OSI-mallin kuljetuskerroksella toimiva tiedonsiirtoprotokolla. Varmistaa että tietoliikennepaketit pääsevät perille ja että ne ovat oikeassa järjestyksessä. Liikenne tapahtuu TCP-session sisällä. |
| TCP RST | TCP Reset. Paketti, jolla TCP-sessio voidaan katkaista. |
| UDP | User Datagram Protocol. Yhteydetön tiedonsiirtoprotokolla. Lähettää paketit, mutta ei varmista niiden perille pääsyä. |
| VLAN | Virtual Local Area Netwok. IEEE 802.1Q standardin määrittelemä tekniikka, jolla voidaan luoda useita loogisia verkkoja saman fyysisen verkon sisään. |
| XML | Extensible Markup Language. Rakenteellinen kuvauskieli. |

# 1. JOHDANTO

Verkkohyökkäysten määrät ja hyökkäysnopeus kasvavat jatkuvasti. Symantecin vuosittaisen Internet Security Threat -raportin mukaan vain tunteja Heartbleed-haavoittuvuuden julkistamisen jälkeen sen käyttö verkkohyökkäyksissä yleistyi merkittävästi [1]. Jos yrityksessä on satoja tai tuhansia haavoittuvia kohteita, vaatii kaikkien kohteiden korjaus todennäköisesti enemmän aikaa kuin muutaman tunnin. Tästä syystä olisikin kätevää, jos yksi yksittäinen laite voisi suojata kaikki haavoittuvat kohteet kerralla. Hyökkäyksenhavainnointi- (IDS) tai hyökkäyksenestojärjestelmä (IPS) on yksi mahdollinen vastaus tällaiseen ongelmaan.

## 1.1 Motivaatio

Hyökkäyksenestojärjestelmiä on ollut olemassa pitkään, mutta kynnys sellaisen käyttöönottoon voi yrityksessä olla korkea, sillä siihen liittyy kustannuksia, ja siitä saatuja hyötyjä on vaikea osoittaa.McAfeen Critical Infratructure Readiness -raportti toteaa, että 625 yritykselle osoitetun kyselyn mukaan monet yritysjohtajat ovat hyvin luottavaisia yrityksiensä hyökkäysten torjunnan nykyiseen tilaan [2]. Samaan aikaan erilaisista tietomurroista uutisoidaan yhä useammin, ja vakavan kyberhyökkäyksen todennäköisyyttä pidetään yhä suurempana [2].

Hyökkäyksenestojärjestelmä ei yksistään tarjoa riittävää turvaa hyökkäyksiä vastaan. Sen avulla voidaan kuitenkin havaita ja estää hyökkäyksiä, joita tavallinen palomuuri ei havaitse. Palomuuri estää yhteyksiä lähinnä liikenteen lähde- ja kohdeosoitteiden ja lähde- ja kohdeporttien perusteella, eikä näin ollen pysty havaitsemaan avatussa portissa tapahtuvaa haitallista toimintaa. Hyökkäyksenestojärjestelmä pystyy analysoimaan liikennettä tarkemmin, ja se voi havaita esimerkiksi protokollatason väärinkäytöksiä, kuten esimerkiksi Ping of Death -hyökkäyksen [3].

Yrityksen verkkoinfrastruktuuriin kohdistuvista hyökkäyksistä ei välttämättä jää jälkeä muualle kuin kohdepalvelun lokeihin. Jos yrityksellä on hallinnassaan useita julkisiin verkkoihin näkyviä sovelluksia, on niihin kohdistuvista uhista vaikeaa saada kokonaiskuvaa, jos tieto niihin suunnatuista hyökkäyksistä on hajallaan tai puuttuu kokonaan. IDS- ja IPS-järjestelmät voivat kerätä tietoa havaituista ja estetyistä hyökkäyksistä ja siten tarjota yritykselle tietoa siitä, millaisia uhkia verkosta kohdistuu.

Nykyään myös tietyt tietoturvastandardit edellyttävät IDS- tai IPS-järjestelmän olemassa oloa. Tällainen on esimerkiksi maksukorttijärjestöjen, kuten Visa Internationalin,

MasterCardin ja American Expressin perustaman PCI Security Standards Councilin luoma PCI-DSS-standardi[4].

## 1.2 Tavoitteet

Yritykset voivat hyödyntää IPS-järjestelmää myös asiakasjärjestelmiensä suojaamiseen omien järjestelmiensä ohella. Tällöin hankintaan, käyttöönottoon ja ylläpitoon liittyvät kustannukset on helpompi perustella, koska asiakkaista voi löytyä myös tahoja, jotka eivät vielä luota nykyiseen suojaukseen verkkohyökkäyksiä vastaan ja ovat valmiita maksamaan lisäturvasta. Nykyään erilaisten IoT-laitteiden ja maksupäätteiden yleistyessä tällaisten asiakkaiden määrä tulee todennäköisesti lisääntymään.

Tämän työn tarkoituksena on ottaa käyttöön IPS-järjestelmä ja suunnitella, miten sen avulla voidaan suojata yrityksen konesalissa toimivia palveluita. Nämä palvelut voivat olla joko yrityksen omia tai sen asiakkaiden palveluita. Pääpaino on kuitenkin asiakkaiden palveluiden ja järjestelmien suojaamisessa ja IPS:n toiminnan tuotteistuksessa tähän tarkoitukseen.

## 1.3 Rakenne

Luvussa kaksi käsitellään IDS- ja IPS-järjestelmiä yleisellä tasolla. Siinä esitellään komponentit, joista järjestelmät muodostuvat, millä tavoin ne toimivat ja miten niitä hallitaan. Luvussa kolme pureudutaan tarkemmin hyökkäyksenestojärjestelmien ominaisuuksiin, ja siihen miten ne vaikuttavat asiakasjärjestelmien suojaamiseen. Luvussa neljä tehdään lyhyt katsaus markkinoilla oleviin IPS-tuotteisiin, ja käsitellään niihin kohdistuvia teknisiä, lainsäädännöllisiä ja muita rajoitteita. Lopulta luvussa viisi päästää käsittelemään tämän työn puitteissa muodostettua IPS-tuotetta, ja sen suunnittelua ja konfigurointia. Samalla otetaan kantaa myös tuotteen jatkokehitykseen ja elinkaareen. Luvussa kuusi esitetään yhteenveto.

# 2. HYÖKKÄYKSEN ESTÄMINEN JA HAVAINNOINTI

IDS- ja IPS-järjestelmät ovat kehittyneet rinnakkain palomuurien kanssa. Näiden järjestelmien toiminta perustuu liikenteen valvontaan tietyissä kohdissa verkkoa. Verkosta yritetään havaita erilaisiin hyökkäyksiin tai väärinkäytöksiin liittyvää liikennettä analysoimalla järjestelmän läpi kulkevia paketteja. IDS- ja IPS-järjestelmistä voidaan puhua yhteisellä IDPS kattotermillä.[5]

Varhaisimpana tunkeutumisen havainnointina voidaan pitää järjestelmässä olevien käyttäjien toimia reaaliajassa valvovaa ylläpitäjää. Tästä seuraavana asteena on järjestelmän tulostettuja lokeja läpikäyvä ylläpitäjä, joka yrittää havaita lokista hyökkäyksiin tai väärinkäytöksiin liittyviä piirteitä. 90-luvun alkuun mennessä lokien läpikäyntiä oli saatu automatisoitua, jolloin alkeellinen IDS-järjestelmä teki sen ja raportoi löydöksistä reaaliaikaisesti. [6]

Nykyiset IDS-järjestelmät voivat tarkkailla tietyn pisteen kautta kulkevaa liikennettä ja siten seurata useisiin järjestelmiin kohdistuvaa liikennettä samanaikaisesti Niiden ei myöskään tarvitse tukeutua järjestelmien lokeihin, vaan esimerkiksi verkkoliikenne voidaan ohjata kulkemaan suoraan IDS-sensorin kautta. Tarvittaessa myös vain kopio liikenteestä voidaan ohjata sensorille. Tällöin IDS:n ongelmat eivät pääse vaikuttamaan liikenteen kulkemiseen kohdepalvelimelle. IPS-jäjestelmä poikkeaa IDS-järjestelmästä siten, että se IPS pystyy itsenäisesti reagoimaan havaittuun uhkaan, ja tarvittaessa estämään liikenteen. IDS pystyy aina vain raportoimaan havainnoistaan.

Niin sanotuista uuden sukupolven palomuureista (NGFW, Next Generation Firewall) alettiin puhua 2010-luvun vaihteessa [7]. Karkeasti ottaen näillä tarkoitetaan palomuuria, johon on yhdistynyt paljon IDS- ja IPS-järjestelmien toiminnallisuutta. Tarkkaa määritelmää termille ei ole, ja eri valmistajat määrittelevät asian eri tavoin. Keskeisintä on, että aiemmin ainoastaan lähde- ja kohdeporttien ja -osoitteiden mukaan liikenteeseen puuttunut palomuuri pystyy nyt prosessoimaan myös sovellustason dataa.

## 2.1 Käyttökohteet

IDPS-järjestelmien tärkein käyttötarkoitus on tunnistaa erilaisia tietoon tai tietojärjestelmiin kohdistuvia uhkia tai tietoturva-, käyttö- tai muiden politiikkojen väärinkäytöksiä. Uhkan tai väärinkäytöksen aiheuttajana voi olla haittaohjelma, hyökkääjä, väärin toimiva ohjelmisto tai inhimillinen virhe. Kun IDPS-järjestelmä havaitsee tällaisen ti-

lanteen, se voi raportoida tilanteesta tietoturvasta vastaaville tahoille, jotka voivat suorittaa mahdolliset jatkotoimenpiteet. IDPS voi myös kerätä tapahtuneesta lokitietoja, jotta tapahtunut voidaan tarkemmin analysoida ja tapahtumasta voidaan oppia. Liikenteestä voidaan myös yrittää tunnistaa merkkejä käyttöpolitiikkojen rikkomisesta, tai havaita merkkejä hyökkäystä edeltävästä tiedustelusta. [8]

Scarfone et. al. toteaa vielä, että organisaatiot ovat hyödyntäneet IDPS-järjestelmiä muun muassa palomuurisääntöjen auditoinnissa. IDPS on tällöin asetettu monitoroimaan liikennettä, joka olisi pitänyt estää. Jos sellaista havaitaan, palomuurit vuotavat jostain. IDPS:n lokien perusteella voidaan myös arvioida miten usein ja millaisia uhkia organisaation verkkoon kohdistuu. Näistä syistä jokaisen organisaation tulisi Scarfonen ym. mukaan harkita IDPS-järjestelmän käyttöönottoa. [8]

## 2.2 Uhkien havainnointitekniikat

IDPS-järjestelmät pyrkivät haivaitsemaan uhkia pääsääntöisesti kahdella eri tavalla, joko tunnisteisiin pohjatuen(signature based) tai etsimällä tietoliikenteestä poikkeamia muodostettuun normaalitilanteeseen nähden (anomaly based). Kolmas käytetty tapa on tilallinen protokolla-analyysi (stateful protocol analysis), joka pyrkii etsimään poikkeuksia tiettyihin protokolliin liittyvissä viesteissä. Yleisimmin käytössä olevat järjestelmät ovat tunnistepohjaisia, mutta joissakin on myös poikkeamapohjaisia komponentteja [9].

### 2.2.1 Tunnistepohjaiset IDPS-järjestelmät

Tunnistepohjaisella IDPS-järjestelmällä on käytettävissä laaja tietokanta erilaisten hyökkäysten tunnisteista. Esimerkiksi Ciscon tietokannassa on tällä hetkellä hieman yli 9000 tunnistetta [10]. Yksittäinen tunniste sisältää tunnusmerkkejä tietynlaisesta verkkoliikenteestä, esimerkiksi tietoa paketin lähde- ja kohdeporteista, protokollan tyypistä tai paketin tietynlaisesta kuormasta.

Toiminnaltaan tunnistepohjainen järjestelmä tarkistaa jokaisen sen läpi kulkevan paketin ja vertaa sitä tunnistetietokantaansa. Jos paketti vastaajotakin tietokannan tunnistetta, IDS reagoi tapahtuneeseen etukäteen määritellyllä tavalla. IDS:n tapauksessa tämä reagointi voi olla tapahtumasta hälyttämistä eri tavoin tai ainoastaan tapahtuneen kirjaaminen lokiin. IPS voi puolestaan myös estää tunnistetta vastaavan liikenteen

Tunnistepohjaisten IDPS-järjestelmien suurin heikkous on, että ne vaativat aiemman hyökkäyksen pohjalta laaditun tunnisteen hyökkäyksestä. Toisin sanoen tunnistepohjaiset järjestelmät eivät pysty reagoimaan millään tavalla täysin uudenlaisiin hyökkäyksiin, kuten nollapäivähaavoittuvuuksiin. Toisena merkittävänä ongelmana on, että vaikka tiettyä liikennettä vastaava tunniste löytyisikin tietokannasta, se ei kaikissa tilanteissa

ole vielä varma merkki hyökkäyksestä. Kolmanneksi ongelmaksi nousee järjestelmän suorituskyky, koska tunnistepohjainen järjestelmä edellyttää, että jokaista pakettia verrataan tietokannan tunnisteisiin[9]. Mikäli liikennettä kulkee IDPS-järjestelmän läpi enemmän kuin järjestelmä pystyy prosessoimaan, on mahdollista, että hyökkäyksiä pääsee silti huomaamatta järjestelmän läpi. Tunnistepohjainen järjestelmä ei myöskään pysty seuraamaan tilallisia yhteyksiä tarkasti [8]. Sillä ei ole tietoa, millä tavalla sovelluksen pitäisi vastata tietynlaiseen viestiin tietyssä vaiheessa kommunikointia. Tunnistepohjainen järjestelmä ei siis voi tunnistaa useista tapahtumista koostuvaa hyökkäystä, jos mikään yksittäinen tapahtuma ei itsessään täytä hyökkäyksen tunnusmerkkejä [8].

### 2.2.2 Poikkeamapohjaiset IDPS-järjestelmät

Poikkeamapohjainen IDPS-järjestelmä luo havaitusta liikenteestä profiilin, jonka avulla se muodostaa vertailutason vastaisuudessa tulevalle liikenteelle [8]. Tämän jälkeen se tarkkailee pakettivirtoja, jotka poikkeavat tästä vertailutasosta. Tällaisia poikkeamia voivat olla esimerkiksi ICMP-pakettien määrän merkittävä kasvu, yhdestä osoitteesta lähetetyn sähköpostin määrän kasvu tai vaikkapa suuri määrä kirjautumisyrityksiä tietyllä palvelimella.

Poikkeamapohjaisen järjestelmän vahvuutena on se, että se ei edellytä mitään aikaisempaa tietoa hyökkäyksistä. Siten tunnistepohjaisen järjestelmän kaltaista tietokantaa tai pakettien erityisen tarkkaa tarkastelua ei tarvita[9]. Toisaalta, joissain tilanteissa on hyvin vaikeaa erottaa normaali liikenne jollain tapaa poikkeavasta liikenteestä. REityisesti uudenlaista liikennettä tuottavaasovellusta käyttöönotettaessa poikkeamapohjaiset järjestelmät voivat tuottaa vääriä hälytyksiä [9].

Poikkeamapohjaisen järjestelmän käyttöönoton jälkeen järjestelmä muodostaa normaaliksi katsotusta liikenteestä profiilin. Tämä vaihe voi olla hyvin pitkä ja toimivan profiilin syntymiseen voi mennä jopa viikkoja [8]. Kun profiili on kerran muodostettu, sitä voidaan käyttää joko staattisena tai dynaamisena profiilina[8]. Staattisen profiilin tapauksessa profiilin tila jäädytetään ja siihen ei tehdä enää muutoksia profiilin käyttöaikana. Dynaamiseen profiiliin taas kerätään jatkuvasti uutta dataa ja se mukautuu uudenlaiseen liikenteeseen. Molemmissa tavoissa on omat heikkoutensa. Koska järjestelmät ja verkot muuttuvat ajan myötä, staattinen profiili ei enää ajan kuluttua vastaa todellista todellisuutta. Dynaamista profiilia taas on mahdollista hämätä esimerkiksi syöttämällä sinne aluksi pieniä määriä haittaliikennettä, ja nostaa määrää pikkuhiljaa ylöspäin, jolloin profiili ehtii mukautua siihen eikä havaitse isoja poikkeamia [8].

Poikkeamapohjaiset järjestelmät voivat siis saada kiinni haittaliikennettä, jota tunnistepohjaiset eivät huomaa. Ongelmana on, että verkkoliikenteeseen täysin sopivan profiilin luominen on hyvin vaikeaa. Tästä syystä poikkeamapohjaiset järjestelmät tuottavatkin yleensä enemmän vääriä positiivisia [8]. Näitä voi aiheutua yksistään jo harvakseen

tehdyistä huoltotöistä, joista aiheutuu poikkeavaa liikennettä. Myös tietyn hälytyksen toteaminen oikeaksi tai vääräksi positiivisesti voi olla hankalaa johtuen kompleksisesta liikenteen käsittelystä. Poikkeamapohjaisissa järjestelmissä voi olla vaikeaa määrittää, miksi tietty hälytys on ylipäätään tapahtunut[8].

### 2.2.3 Tilallinen protokolla-analyysi

Tilallinen protokolla-analyysi on tekniikka, jolla IDPS pyrkii havainnoimaan vääriä tai epäilyttäviä tapoja tietoliikenneprotokollien käytöstä liikenteessä. Vertailutaso on yleensä muodostettu protokollien RFC-dokumenttien perusteella. Eri IDPS-tekonologiat käyttävät tästä ominaisuudesta eri nimiä, ja esimerkiksi Ciscon tapauksessa Deep Packet Inspection yksi tilallisen protokolla analyysin toteutus[11].

Tilallisen protokolla-analyysin tarkastelulla voidaan havaita esimerkiksi tietyn paketin poikkeuksellinen toistuminen,tai että pakettia, josta havaitun paketin toiminnallisuus riippuu, ei ole havaittu. Koska tarkastelu on tilallista, IDPS pystyy arvioimaan liikennettä istuntokohtaisesti ja huomiomaan tilanteet, joissa itsessään luvallisia paketteja liikkuu, ilman että niitä edeltäviä paketteja on havaittu. Tilallisella protokolla-analyysilla IDPS voi myös pitää kirjaa sessioon liittyvästä käyttäjästä, ja siten esittää esimerkiksi tilastoa tietyn käyttäjän toimista pidemmältä aikaväliltä. [8]

Tilallisen protokolla-analyysin suurin heikkous on sen raskaus. Useiden istuntojen pitäminen muistissa ja istuntoihin kuuluvien pakettien monipuolinen ja tarkka tarkastelu vaatii laitteistolta paljon resursseja. Toinen ongelma on ohjelmistotuottajien omat, RFC:stä poikkeavat, tulkinnat protokollien toiminnasta. IDPS voi tulkita tällaisen vastoin RFC:n määritelmiä toimivan protokollan hyökkäykseksi tai muuksi väärinkäyttöyritykseksi. [8]

## 2.3 IDPS-sensorin sijoittelu

IDPS-järjestelmien toiminta perustuu verkkoliikennettä tarkkailevaan sensoriin. Tämä sensori voi olla joko kokonaan erillinen komponenttinsa verkkotopologiassa, tai sitten se voi sijaita suoraan päätelaitteella. Sensorin sijoittelun perusteella IDPS-järjestelmät voidaankin jakaa kolmeen tyyppiin

- Päätelaiteperustaiset (Host-Based): Tarkkaillaan yhden päätelaitteen tapahtumia hyökkäysten tai muiden väärinkäytösten varalta. Voidaan tarkkailla verkkoliikennettä, järjestelmän lokeja, ajossa olevia prosesseja, tiedostojen käyttöä ja muutoksia yms. Tällaisia sensoreita kannattaa käyttää lähinnä kriittisimmissä tai hyökkäyksille alttiimmissa laitteissa. [8]

- Verkkoperustaiset (Network-Based): Tarkkaillaan tiettyjen verkkoblokkien tai -laitteiden välistä liikennettä. Analysoidaan verkko- ja sovellusprotokollien aktii-

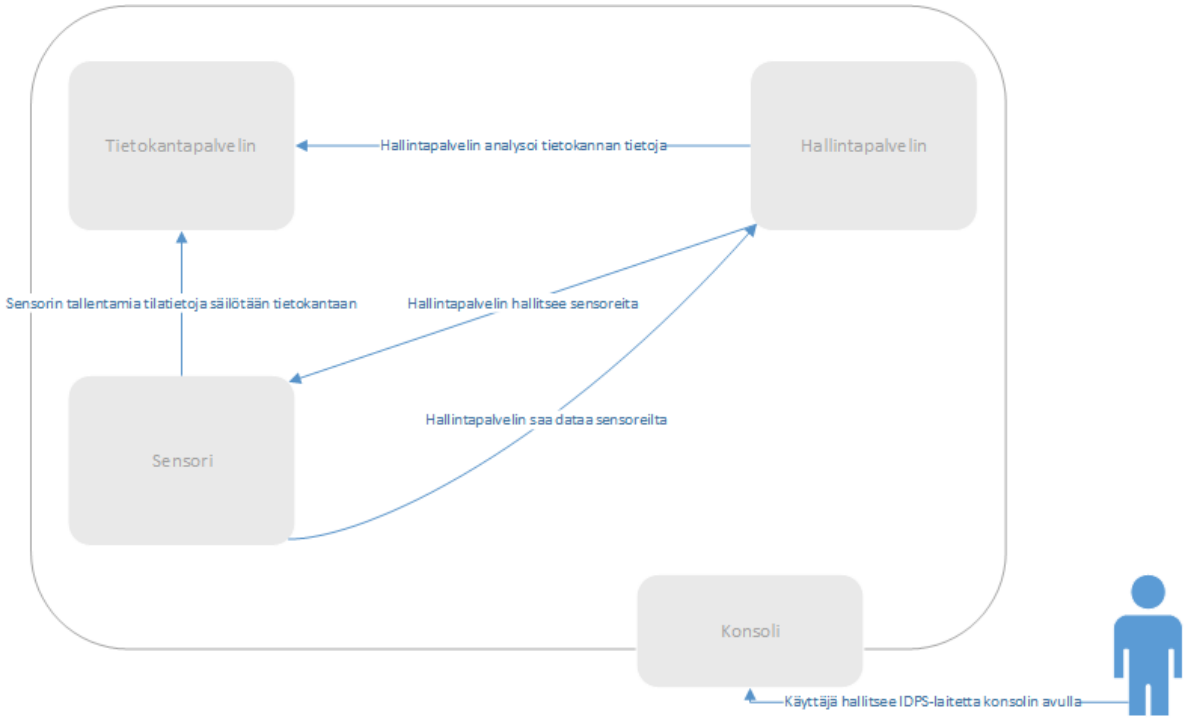
visuutta, ja yritetään merkkejä väärinkäytöstä. Tällainen sensori on yleisimmin käytössä verkkojen rajalla eli esimerkiksi organisaation reunareitittimen yhteydessä. [8]

- Hybridit: Näissä käytetään molempia sekä päätelaiteperustaista että verkkoperustaista IDPS-järjestelmää. [5]

Näiden lisäksi Scarfone ym. nimeää IDPS-järjestelmien yhdeksi tyypiksi verkon käyttäytymisanalyysiin (Network Behaviour Analysis) perustuvat järjestelmät. Näitä järjestelmiä käytetään yleensä sisäverkon liikenteen tarkkailuun, jolloin ne yrittävät havaita epätavallisia liikennevirtoja, kuten merkkejä haittaohjelmien liikenteestä tai palvelunestohyökkäyksistä.

## 2.4 Järjestelmien komponentit

IDPS-järjestelmän voidaan katsoa muodostuvan komponenteista, jotka kukin toteuttavat osan järjestelmän toiminnallisuudesta. Toimintojen jakautumisesta eri komponentteihin löytyy muutama erilainen näkemys. Tämän dokumentin puitteissa käytetään kuitenkin Scarfornen ym. esittämää mallia, jossa järjestelmä jakautuu neljään erilliseen komponenttiin [8]. Nämä komponentit voivat joissain tilanteissa olla samassa laitteessa tai sovelluksessa tai ne ovat eriytetty omiksi laitteikseen. Kuvassa yksi esitetään tämän mallin perusteella piirretty kuva komponenteista ja niiden vuorovaikutuksista.



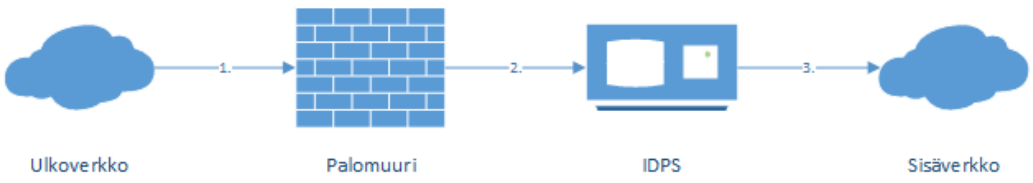

***Kuva 1.*** *IDPS-järjestelmän komponentit*

Mallin mukaiset komponentit ovat siis seuraavat:

- Sensori: Sensori valvoo ja analysoi liikennettä. Päätelaiteperustaisissa laitteissa sensoria kutsutaan usein agentiksi.
- Tietokantapalvelin: Sensorit tallentavat tapahtumatietoja tietokantaan.
- Hallintapalvelin: Keskitetty laite, joka analysoi sensorien ja agenttien tuottamaa tietoa. Yksi hallintapalvelin voi siis hallita useampaa sensoria tai agenttia. Se voi myös yrittää yhdistää eri agenteilta saatua dataa ja muodostaa siten paremman kokonaiskuvan yksittäisestä tapahtumasta. Kaikissa IDPS-järjestelmissä ei välttämättä ole erillistä hallintapalvelinta, mutta suuremmissa kokonaisuuksissa niitä voi olla useita.
- Konsoli: Konsoli on käyttäjien ja ylläpitäjien rajapinta järjestelmään. Se tarjoaa yleensä sekä hallinta- että valvontamahdollisuudet.

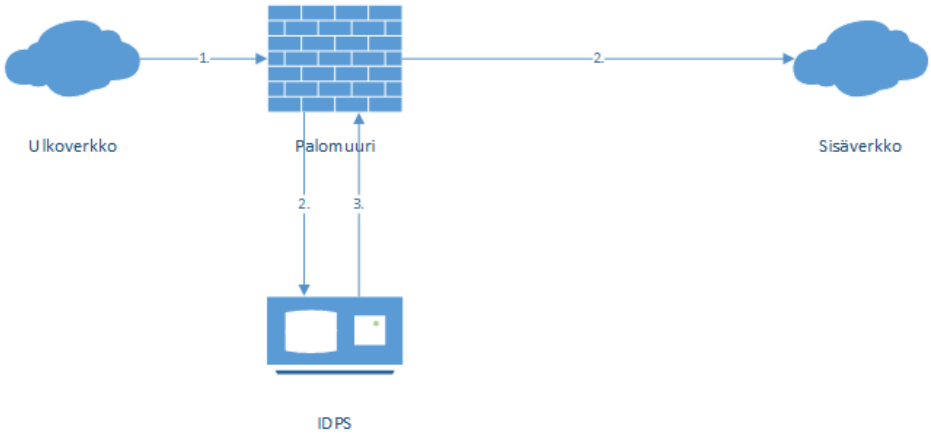
## 2.5 IDPS-järjestelmän sijoitus verkkotopologiaan

IDPS -järjestelmät voidaan sijoittaa verkkoon suoraan liikennevirtaan. Laite sijaitsee tällöin joko fyysisesti tai loogisesti ulkoverkon ja sisäverkon välissä, ja kaikki sisäverkkoon tuleva liikenne kulkee IDPS-järjestelmän läpi. Tämä tilanne on kuvattu kuvassa 2. Liikenne kulkee palomuurilta IDPS-laitteelle, joka tarkastelee sitä halutulla tavalla ja sitten päästää sallitun liikenteen jatkamaan normaalisti sisäverkkoon. Yleensä vain osa liikenteestä halutaan viedä IDPS:n läpi, joten liikenne voidaan palomuurilta ohjata myös IDPS:n ohi suoraan sisäverkkoon. Tässä mallissa on huomioitavaa, että IDPS:n kautta kulkemaan ohjattu liikenne ei missään tilanteessa pääse kulkemaan sen ohi.



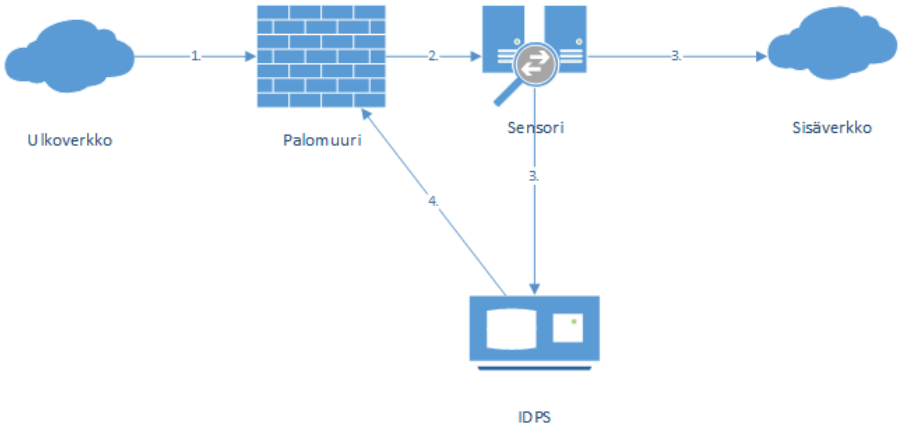

***Kuva 2.*** *Suoraan liikennevirtaan sijoitettu IDPS*

Toinen vaihtoehto on kuvassa 2 esitetty tilanne, jossa laite on sijoitettu muualle verkkoon, ja kopio halutusta liikenteestä on ohjattu myös IDPS:lle. Tässä tilanteessa palomuurin läpäissyt liikenne ohjataan sekä IDPS:lle, että suoraan sisäverkkoon. Kun IDPS on prosessoinut vastaanottamansa liikenteen, se ohjaa palomuuria toimimaan halutulla tavalla lopun liikenteen suhteen. Tällöin IDPS ei pysty reagoimaan yhtä nopeasti havaittuihin poikkeamiin, mutta toisaalta laitteen omat resurssit ja mahdollinen hajoaminen eivät vaikuta muun liikenteen kulkemiseen.




***Kuva 3.*** *Liikennevirran ulkopuolelle sijoitettu IDPS*

Molemmat edellä esitellyt topologiat on mahdollista toteuttaa myös tilanteessa, jossa käytetään IDPS-laitteesta erillistä sensoria. Tällainen tilanne on kuvassa neljä. Tällainen ratkaisu tuo joustavuutta IDPS:n arkkitehtuuriin ja mahdollistaa useiden sensorien käytön samassa järjestelmässä. Erillinen sensori lisää kuitenkin järjestelmän kokonaisviivettä, koska kommunikointiin sensorin ja IDPS-järjestelmän välillä kuluu enemmän aikaa. Kokonaisviiveen muodostumista on käsitelty tarkemmin luvussa 3.4.




***Kuva 4.*** *Liikennevirtaan sijoitettu sensori*

IDPS-sensori on mahdollista sijoittaa myös liikennevirran ulkopuolelle, jolloin sen analysoitavaksi tulee ainoastaan kopio liikenteestä ja sen toiminnan häiriöt eivät vaikuta suojattujen palveluiden käytettävyyteen. Tämä tosin lisää järjestelmän sisäistä viivettä entisestään, sillä aikaa kuluu sekä liikenteen siirtymiseen sensorille että sensorin ja IDPS:n väliseen kommunikaatioon.

IDPS:n sijoituksessa verkkotopologiaan on siis aina kyse kompromissista vasteen nopeuden ja vikasietoisuuden välillä. Erilliset sensorit voivat lisätä järjestelmän joustavuutta ja ne mahdollistavat useiden pisteiden kautta kulkevan liikenteen analysoinnin samalla IDPS-teknologialla.

## 2.6 Valmiudet

IDPS-järjestelmällä on valmiuksia toimia erilaisissa tilanteissa. Scarfone ym. jakaa IDPS-järjestelmien valmiudet neljään luokkaan: havainnointi-, lokien keräys-, tunnistus- ja estovalmiudet [8].

### 2.6.1 Havainnointi

Tärkein IDPS:n ominaisuus on havainnointi. Ilman sitä muut toiminnallisuudet eivät olisi mahdollisia. IDPS-järjestelmät keräävät tietoa verkossa havaituista järjestelmistä, niiden generoimasta ja niille kulkevasta liikenteestä, ja liikenteen käyttämistä porteista.

### 2.6.2 Lokien kerääminen

IDPS-järjestelmä pystyy laatimaan keräämästään tiedosta lokia. Kerättävät lokitiedotriippuvat IDPS-järjestelmän tyypistä. Päätelaiteperusteiset järjestelmät voivat kerätä lokia esimerkiksi laitteen käyttäjistä ja käyttäjänimistä, kun taas verkkoperusteiset pääsevät käsiksi useiden lähde-kohde-parien väliseen liikenteeseen. Kaikki laitteet pääsääntöisesti keräävät lokiinsa tapahtuman aikaleiman, tapahtuneen prioriteetin ja IPS:n tapauksessa, tapahtuman vuoksi suoritetut toimet. Lokit kannattaa säilyttää sekä paikallisesti IDPS-laitteistossa että keskitetyllä lokien keräämiseen tarkoitetulla palvelimella, kuten syslog-palvelimella. Tällä varmistetaan lokien eheys ja saatavuus, mikäli IDPS-järjestelmä altistuisi hyökkäykselle. Lokeja keskitettäessä on syytä varmistaa, että kaikkien laitteiden kellot ovat samassa ajassa, jotta kerätyn datan eheys säilyy. Tämä voidaan tehdä esimerkiksi NTP-protokollaa käyttämällä. [8]

### 2.6.3 Tunnistus

Tunnistuksella tarkoitetaan IDPS-järjestelmän kykyä tunnistamaan uhkia keräämästään datasta [12]. Yksi järjestelmä käyttää yleensä useampaa kohdassa 2.2 esiteltyä havainnointitekniikkaa, niin saavutetaan parempia tuloksia uhkien havainnoinnissa. Tunnistusparametreja on IDPS-järjestelmän käyttöönotossa syytä muokata kulloiseenkin tilanteeseen sopivaksi. Lähtökohtaisesti voidaan sanoa, että yksikään IDPS-järjestelmä ei toimi optimaalisesti oletusasetuksilla. Muun muassa seuraavia tunnistusominaisuuksia voidaan järjestelmissä yleensä muokata:

- Kynnysarvot: Montako kertaa tietty tapahtuma voi tapahtua aikayksikköä kohden ennen kuin se on poikkeuksellista? Kynnysarvoilla määritellään rajoja normaalin ja poikkeavan toiminnan väliin. Näitä käytetään yleensä poikkeamapohjaisissa ja tilallista protokolla-analyysia käyttävissä järjestelmissä.
- Mustat ja valkoiset listat: Musta lista voi sisältää esimerkiksi joukon IP-osoitteita tai muita tunnistetietoja, joista tiettyä tapahtumaa ei missään tapauksessa sallita. Valkoisen listan kohteet toimivat taas päinvastoin, ja niihin osuvat

tapahtumat sallitaan. Valkoiset listat sopivat erityisesti toistuvasti havaittujen väärien positiivisten käsittelyyn, jotta turhia hälytyksiä saadaan karsittua. Molempia listoja käytetään erityisesti tunnistepohjaisten ja tilallista protokolla-analyysia käyttävien järjestelmien kanssa.

- Hälytysasetukset: Mistä kaikesta IDPS-järjestelmä hälyttää, minkä tasoisesella hälytyksellä, ja aiheutuuko hälytyksestä muita toimia? IDPS-järjestelmät ilmoittavat havaitsemistaan uhkista hälytyksillä.

Näiden lisäksi tunnistukseen vaikuttaa käytettävissä olevan IDPS-järjestelmän tunnistusmoottori. Avoimen lähdekoodin järjestelmissä tätä on mahdollista itsekin muokata ja parannella kooditasolla, mutta kaupallisissa järjestelmissä se tapahtuu yleensä järjestelmän toimittajan puolelta.

### 2.6.4 Estäminen

IPS-järjestelmät voivat pelkän havainnoinnin lisäksi myös estää liikennettä. Estotoimien konfigurointiin kannattaa käyttää riittävästi aikaa, sillä huonosti konfiguroidut IPS-järjestelmät voivat aiheuttaa paljon haittaa järjestelmien normaalille toiminnalle. Yleensä IPS-järjestelmää kannattaakin aluksi käyttää pelkässä IDS-moodissa, jolloin se ei estä liikennettä, mutta generoi hälytyksiä normaalisti. Tällä tavoin on mahdollista hienosäätää järjestelmän toimintaa riittävästi, ennen kuin sen esto-ominaisuuksia otetaan käyttöön.Erilaisia IPS-järjestelmän tarjoamia estotoimia on kuvattu tarkemmin luvussa 2.7.

## 2.7 IPS:n suorittamat vastatoimenpiteet

Tavat, joilla IPS-järjestelmä voi reagoida havaittuun hyökkäykseen, voidaan luokitella neljään eri ryhmään sen mukaan, mihin protokollapinon kerrokseen ne vaikuttavat. Huomion arvoista on, että tässä yhteydessä sovelluskerroksella viitataan OSI-mallin istunto, esitystapa- ja sovelluskerroksiin. [12]

Seuraavissa aliluvuissa on käsitelty IPS:n vastatoimia eri protokollapinon kerroksilla. Lähtökohtana on, että alemmalla tasolla IPS vastatoimen suorittaa, sitä edullisempaa se on järjestelmälle ja sitä vähemmän laitteen resursseja se kuluttaa. IPS:n näkökulmasta on siis edullisempaa estää liikennettä tiettyjen lähde- ja kohdeosoitteiden välillä, kuin muokata näiden välillä kulkeva sovelluskerroksen data vaarattomaksi.

### 2.7.1 Siirtokerros

Tällä kerroksella toimiessa IPS-järjestelmä ei suoranaisesti voi itse estää haittaliikennettä. Rash ym. toteavat, että IPS voi kuitenkin ilmoittaa hyökkäyksestä, jolloin järjestelmän ylläpitäjät voivat sulkea hyökkäyksen lähdeportin tai estää liikenteen muulla tavoin. Tämä on mahdollista ainoastaan, jos hyökkäys on käynnistetty paikallisesta järjes-

telmästä. Useimmiten IPS:n havaintojen vuoksi tehdyt porttien sulkemiset halutaan purkaa, kun hyökkäys on ohi. Tästä syystä onkin hyvä käyttää jonkinlaista aikakatkaisua luotujen estosääntöjen kanssa. [12]

### 2.7.2 Verkkokerros

IPS-järjestelmä käynnistää toimet, joilla liikenne hyökkääjän IP-osoitteesta estetään. Jos IPS-järjestelmä on sijoitettu suoraan liikennevirtaan, se pystyy itse estämään tällaisen liikenteen. Muussa tapauksessa on mahdollista konfiguroida IPS-järjestelmä estämään vastaava liikenne ohjaamalla reunapalomuuria. Menetelmästä riippumatta luodun säännön kanssa on hyvä käyttää jonkinlaista aikakatkaisua, jonka jälkeen estosääntö poistuu järjestelmistä. [12]

### 2.7.3 Kuljetuskerros

IPS-järjestelmä voi generoida TCP RST paketin, jolla se voi katkaista haitallisen TCP-session, tai vastata haitalliseen UDP-liikenteeseen ICMP-paketilla, jossa jokin tilanteeseen sopiva virhekoodi. Tällä kerroksella ei tarvita aikakatkaisuja, koska vastatoimet tehdään sessio- tai pakettikohtaisesti. [12]

### 2.7.4 Sovelluskerros

Suoraan liikennevirtaan sijoitettu IPS-järjestelmä voi muokata paketeissa kulkevaa haitallista sovellusdataa harmittomaksi, ennen kuin paketit pääsevät kohteeseensa. Jos kuljetuskerroksen kuormana kulkevaa dataa muokataan, täytyy samalla laskea kuljetuskerroksen käyttämä tarkistussumma uudelleen. [12]

## 2.8 IDPS-järjestelmän toiminnan häiritseminen

IDPS-järjestelmillä on omat heikkoutensa. Hyökkääjän täytyykin vain selvittää, minkä tyyppinen hyökkäyksen havainnointi- tai estojärjestelmä vastapuolella on ja valita hyökkäykseen käytettävät menetelmät sen mukaan. Liu ym. jakavat IDPS:n toiminnan häirintä- ja välttelytavat seuraavaan seitsemään luokkaan [13]. Näistä kolme ensimmäistä käytännössä edellyttävät hyökkääjältä pääsyä sensorin ja hallintakonsolin väliseen verkkoon. Loput ovat sellaisia joihin ei hyvällä verkkosuunnittelullakaan voida täysin puuttua.

### 2.8.1 Hyökkäykset hallintakonsolia vastaan

Hallintakonsoli on kriittisin kohta, jota vastaan järjestelmässä voidaan hyökätä. Sen kautta pystytään vaikuttamaan koko järjestelmän toimintaan poistamalla tiettyjä tunnisteita tai sääntöjä käytöstä, tai vaikka sammuttamalla järjestelmä kokonaan. [13]

### 2.8.2 Hyökkäykset sensoria vastaan

Lähtökohtaisesti sensorilla on kaksi verkkoliitäntää, joista toista käytetään liikenteen analysointiin ja toinen kommunikointiin hallintakonsolin kanssa. Liikenteen analysointiin käytettävälle verkkoliitännälle ei yleensä ole annettu IP-osoitetta, joten hyökkäykset sitä vastaan ovat hankalampia toteuttaa. Hyökkääminen hallintaan käytettävään verkkoliitäntään voikin olla helpompi toteuttaa, ja tällöin voidaan yrittää esimerkiksi sensorin haltuunottoa. [13]

### 2.8.3 Välimieshyökkäys

Välimieshyökkäys (Man In the Middle, MITM) kohdistuessaan hallintaan käytettävään verkkoliitäntään on myös hyökkääjän kannalta houkutteleva. Hyökkääjä voi asettua hallintakonsolin ja sensorin väliin ja väärentää liikennettä kumpaan suuntaan tahansa. Tällöin esimerkiksi tietyt hälytykset voidaan jättää raportoimatta hallintakonsolille tai sensori voidaan sammuttaa kokonaan konsolin huomaamatta. [13]

### 2.8.4 Kuormitushyökkäys

Hyökkääjän on mahdollista generoida pienessä ajassa hyvin suuri määrä yleisiin hyökkäyksien tunnisteisiin osuvaa liikennettä. Kun määrä kasvaa riittävän suureksi, IDPS-järjestelmän prosessointikyvyn rajat ja saapuvien pakettien puskuri tulevat täyteen. Tällöin IDPS joko pudottaa seuraavat saapuvat paketit kokonaan tai päästää ne läpi ilman prosessointia. Useimpien IDPS-järjestelmien pitäisi nykyisin pystyä tunnistamaan tämä hyökkäys ja torjumaan sen haitat. [13]

### 2.8.5 Lisäys ja välttely

IDPS-järjestelmäähämätäkseen hyökkääjä voi yrittää lisätä haitallisen datan perään muuta dataa, jolloin data ei enää ole haitallista. Huonosti konfiguroitu IDPS saattaa kuitenkin tunnistaa sen hyökkäykseksi ja tuottaa väärän positiivisen. Välttelyssä taas haitallinen data pyritään naamioimaan siten, että IDPS ei enää tunnista sitä hyökkäykseksi, mutta sen vaikutus kohdejärjestelmään on hyökkääjän tavoittelema. Tässä tapauksessa IDPS tuottaa siis väärän negatiivisen. Lisäykseen ja välttelyyn perustuvat menetelmät ovat uhka erityisesti hyökkäyksien tunnisteisiin perustuvissa IDPS-järjestelmissä. [13]

### 2.8.6 Palvelunestohyökkäys

Palvelunestohyökkäyksellä on mahdollista häiritä sensorin ja hallintakonsolin välistä liikennettä [13]. Tämä eroaa kuormitushyökkäyksestä sikäli, että tarkoituksena ei ole ylikuormittaa sensoria, vaan häiritä sensorin kykyä kommunikoida hallintakonsolille. Yun ym.mukaan tämän voi saada aikaan DOS-hyökkäksillä [14].

### 2.8.7 Tunnelointi ja liikenteen salaus

IDPS-järjestelmät eivät pysty tutkimaan salattua liikennettä. Tämän vuoksi onkin syytä miettiä tarkkaan, mitä salatun liikenteen suhteen halutaan tehdä. Käytännössä salattu liikenne on joko mahdollista päästää läpi tai estää.

## 2.9 IDPS-järjestelmän hallinta

IDPS-järjestelmän hallinta on tämän dokumentin puitteissa jaettu käyttöönottoon ja ylläpitoon. Käyttöönoton yhteydessä valitaan käytettävä IDPS-tuote, sopiva laitteisto ja arkkitehtuuri. Ylläpito ja käyttö-vaiheessa keskitytään järjestelmän päivittäiseen käyttöön ja sen vaatimiin ylläpito toimiin.

### 2.9.1 IDPS-tuotteen valinta

IDPS-tuotteen valinta perustuu organisaation tarpeisiin, joten yleispätevää prosessia tai kriteeristöä sopivan tuotteen valintaan ei ole. Scarfone ym. listaavat kuitenkin joukon yleisiä suosituksia, jotka antavat suuntaa tuotteen valintaan[8]:

- Organisaation verkon ja järjestelmien tunteminen on tärkeää. Halutaanko valvoa koko verkkoa, vain osaa siitä tai vain tiettyjä laitteita? Verkon laajuus ja topologia vaikuttaa tarvittavien sensorien määrään. Mikäli verkossa on jo aiempia IDPS-laitteita, on selvitettävä halutaanko uusilla laitteilla laajentaa vanhojen toimintaa vai korvata se?
- IDPS:n käyttöönotolle on hyvä määritellä selkeät tavoitteet. On syytä arvioida, millaisia uhkia IDPS:llä halutaan torjua, vai halutaanko järjestelmää käyttää enemmänkin sisäisten politiikkojen mukaisen toiminnan valvontaan?
- Organisaation olemassa olevat tietoturvapolitiikat voivat asettaa vaatimuksia tai rajoituksia IDPS-järjestelmälle. Esimerkiksi organisaatiossa voi olla jo olemassa toimintamallit tietoturvarikkomusten käsittelyyn. Näiden mallien toiminta IDPS:n generoimien hälytysten kanssa on syytä suunnitella etukäteen.
- Organisaation käytäntöihin kohdistuvat ulkoiset vaatimukset voivat myös vaikuttaa IDSP-järjestelmän valintaan ja haluttuihin ominaisuuksiin. Paikallinen lainsäädäntö voi itsessään asettaa vaatimuksia järjestelmän valintaan. Muita ulkoisia vaikuttimia ovat esimerkiksi erilaiset tietoturvastandardit, tietoturva-auditointien asettamat vaatimukset ja asiakkailta tulevat vaatimukset.
- IDPS-järjestelmän valintaan vaikuttaa myös organisaation käytössä olevat resurssit. IDPS aiheuttaa kaksi merkittävää kuluerää. Ensimmäinen on itse laitteiston hankinta- ja lisenssikustannukset. Laitteet itsessään ovat yksittäinen kuluerä, mutta ne tarvitsevat yleensä koko elinkaarensa ajaksi lisenssin ja tukisopimuksen. Toisena kulueränä on IDPS:n ylläpitoon kuluva työ, ja tarvittavan osaami-

sen hankinta. Jotkut IDPS-järjestelmät toimivat sillä oletuksella, että henkilöstöä on valmiina valvomaan niiden toimintaa ympäri vuorokauden.

### 2.9.2 Käyttöönotto

Käyttöönottoon liittyvät toimet ovat pääpiirteiltään samat järjestelmästä riippumatta vaikka eri teknologiat tuovat mukanaan omia piirteitään ja rajoituksiaan. Nämä on syytä tuntea ja huomioida käyttöönoton yhteydessä.

Aluksi on syytä suunnitella IDPS-järjestelmän arkkitehtuuri. Scarfone ym. mukaan seuraavat asiat kannattaa huomioida arkkitehtuuria suunnitellessa[8]:

- Sensorien ja agenttien sijoittelu.
- Kuinka luotettava ratkaisu on? Onko jotain komponentteja tarpeen kahdentaa?
- Millaista kuormaa järjestelmän tulisi kestää?
- Mihin muihin järjestelmiin IDPS on yhteydessä? Lähettääkö IDPS lokit keskitetylle palvelimelle? Lähettää IDPS sähköpostia?
- Mitä muutoksia verkkoinfrastruktuuriin täytyy tehdä, jotta IDPS-järjestelmä voidaan ottaa käyttöön?

Scarfone myös suosittaa IDPS-järjestelmän käyttöönottoa ensin testiympäristössä. Tällä tavoin suurimmat ongelmat saadaan todettua ilman tuotantoympäristöön kohdistuvia riskejä. Käyttöönoton tuotantoympäristössä olisi myös hyvä tapahtua vaiheittain, ja järjestelmän estotoimintojen tulisi alkuun olla poissa päältä, jotta väärät positiiviset eivät estä liikenteen kulkua aiheetta. Sensorien käyttöönotto vaiheittain auttaa myös minimoimaan väärien positiivisten määrää. [8]

Käyttöönoton yhteydessä tulisi myös ottaa kantaa siihen, millä tavoin IDPS-järjestelmää tullaan jatkossa hallitsemaan. Teoriassa on mahdollista kytkeytyä hallintaohjelmistolla suoraan IDPS-laitteiden konsoliporttiin, mutta tämä on käytännössä mahdollista vain, jos ylläpitohenkilöstö on samoissa tiloissa IDPS-laitteiden kanssa. Toisinaan IDPS-laitteiden kanssa kannattaa käyttää omaa erillistä hallintaverkkoa [8]. Hallintaverkko on monessa mielessä hyvä ratkaisu. Se voi olla täysin erillinen asiakasliikennettä kuljettavasta verkosta ja julkisista verkoista. Näin ollen se estää IDPS-laitteiden näkymisen julkiverkkoihin täysin ja siten estää ulkoa päin tulevat hyökkäykset. Hallintaverkko mahdollistaa myös pääsyn hallintakonsoliin hyökkäystilanteessa, jossa muut verkot ovat kuormittuneita. Erillisen hallintaverkon ongelmana onkin lähinnä sen lisäämä kompleksisuus. Ollakseen asiakasverkoista täysin erillinen ja riippumaton, hallintaverkon pitäisi olla toteutettu kokonaan omilla laitteillaan.Tällöin esimerkiksi pelkkä VLAN:ien käyttö liikenteen loogiseen erotteluun ei riitä. Kokonaan omien laitteiden käyttö taas lisää verkon monimutkaisuutta merkittävästi. Hallintaverkon eriyttäminen omille laitteille ei välttämättä ole kannattavaa pelkästään IDPS-laitteiden takia. Monikäyttöisin ratkaisu hallintaverkon suhteen lienee asiakas- ja julkiverkoista loogisesti eriytetty verkko, joka

piilottaa IDPS:n olemassaolon ulkopuolisilta, mutta mahdollistaa sen ylläpidon verkon kautta.

### 2.9.3 Ylläpito ja käyttö

IDPS-järjestelmät pääsääntöisesti tarjoavat graafisen käyttöliittymän, jota kutsutaan myös konsoliksi, kuten luvussa 2.4. Yleisimmät hallinta- ja ylläpitotoimet voidaan suorittaa konsolin kautta. Tällaisia ovat muun muassa järjestelmän konfigurointi, päivityksien asentaminen, komponenttien tilan valvonta ja raporttien ja hälytysten konfigurointi. Kaikille konsolin käyttäjille ei voida antaa oikeuksia muokata järjestelmän konfiguraatiota, joten konsoleissa onkin useimmiten mahdollisuus hienojakoiseen käyttöoikeuksien myöntämiseen erillisille käyttäjille. Tällä tavoin jotkin järjestelmät mahdollistavat IDPS-kokonaisuuden jakamisen pienempiin hallittaviin osiin, joilla jokaisella voi olla omat käyttäjänsä, ja nämä käyttäjät näkevät esimerkiksi vain tietyn sensorin datan. Jotkut IDPS:t tarjoavat graafisen käyttöliittymän lisäksi myös komentorivipohjaisen konsolin. Graafisen käyttöliittymän etuna on usein helpompi käyttö, mutta komentorivi voi mahdollistaa toimintoja, joita ei voi käyttää graafisen käyttöliittymän läpi. [8]

IDPS-järjestelmien konsolit yleensä avustavat käyttäjiä päivittäisessä toiminnassa. Ne jäsentelevät tietoa kontekstin mukaan helpommin hallittaviksi kokonaisuuksiksi, ja yrittävät auttaa käyttäjää oikean tiedon etsinnässä. Mitä enemmän dataa IDPS-järjestelmä saa, sen paremman kokonaiskuvan sen avulla pystyy muodostamaan tapahtuneesta. Jotkut järjestelmät osaavat myös itse koota saamastaan datasta tapauksia, joissa kaikki yhteen tapahtumaan liittyvät data on koostettuna. Ne saattavat myös ohjata käyttäjän työnkulkua ja siten helpottaa tapauksen käsittelyä. [8]

Konsolit tarjoavat myös mahdollisuuksia IDPS:n toiminnan raportointiin. Raportteja voidaan generoida automaattisesti ja toimittaa esimerkiksi sähköpostilla vastaanottajille. Käyttäjät voivat myös luoda itse raportteja esimerkiksi tietystä tapauksesta. IDPS voi tarjota mahdollisuuden viedä dataa jossakin yleisessä formaatissa, kuten esimerkiksi CSV-tiedostona. Tämä on hyödyllistä, jos IDPS ei pysty itse käsittelemään dataa tarpeeksi, ja tarvitaan ulkopuolisia järjestelmiä, joissa prosessointia voidaan jatkaa. [8]

IDPS-järjetelmiin on yleensä saatavilla kahdenlaisia päivityksiä. Ohjelmistopäivitykset korjaavat IDPS-järjestelmässä havaittuja ongelmia tai tuovat uusia ominaisuuksia. Nämä voivat koskea vain osaa IDPS:n komponenteista tai niitä kaikkia, ja näiden asentaminen vaatii yleensä päivitettävän IDPS-komponentin tai koko järjestelmän uudelleenkäynnistyksen. Toinen IDPS:ssä päivittyvä asia ovat tunnisteet. Tunnistepäivitykset sisältävät tietoa uusista uhista ja haavoittuvuuksista, joille IDPS-tuoteen toimittaja on laatinut sopivat tunnisteet. Molempien päivitysten asennus on tyypillisesti suunniteltu siten, että tunnisteisiin käyttäjien puolesta tehty hienosäätö ja muut konfiguraatiomuutokset säilyvät päivityksistä huolimatta. On kuitenkin suositeltavaa varmuuskopioida

konfiguraatio ennen päivityksiä ja lisäksi testata päivitysten toiminta testiympäristössä ennen tuotantoympäristön päivitystä. [8]

Ylläpitäjillä ja käyttäjillä tulee olla riittävät tiedot ja osaaminen IDPS-järjestelmän käyttöön. IDPS-järjestelmien yleisimpiä periaatteita voi opiskella kirjoista, artikkeleista ja muista teknisistä dokumenteista. Jokainen IDPS-tuote on kuitenkin erilainen ja on hyvä hankkia mahdollisimman paljon tietoa myös juuri käyttöönotettavasta järjestelmästä. Scarfone ym. listaa joukon lähteitä, joista tällaista tietoa voi hankkia [8]:

- Tuotteen valmistajan koulutukset. Useimmat valmistajat tarjoavat koulutuksia tuotteidensa käyttöön. Koulutuksissa käyttäjät pääsevät itse tutustumaan laitteisiin testiympäristössä kouluttajan kertoessa asiasta ja vastatessa kysymyksiin.
- Tuotteen dokumentaatio. Monilla tuotteilla on hyvin kattavat käyttöohjeet ja erilliset ohjeet asennukseen, käyttöön ja hallintaan. Dokumentaatiosta voi löytyä myös valmistajan omia suosituksia laitteiden käyttöön.
- Tekninen tuki. Valmistajan tarjoama tekninen tuki yleensä joko kuuluu tuotteen hankintahintaan tai lisenssi kustannuksiin, tai on saatavissa erillisellä sopimuksella. Tukea voidaan käyttää ongelmien ratkomiseen, ja vastaamaan tuotetta koskeviin kysymyksiin.
- Valmistajan konsultointi. Jotkut valmistajat tarjoavat maksullista konsultaatiota tilanteisiin, jotka ovat tuen ja koulutuksien ulkopuolella. Tällaisia voivat olla esimerkiksi sopivan tunnisteen luominen tai IDPS:n hienosäätö asiakkaan tarpeisiin.
- Käyttäjäyhteisöt. Yleisimpien tuotteiden ympärille on muodostunut käyttäjäyhteisö, joka kommunikoi keskenään esimerkiksi foorumien kautta. Toisilta käyttäjiltä voi pyytää apua tai tarjota sitä itse. Saatuun tietoon kannattaa kuitenkin suhtautua varauksella, ja on syytä varoa mitä tietoa itse paljastaa yrityksen järjestelmistä.

## 2.10 IDPS:n testaus

IDPS-järjestelmän testaus ei ole aivan yksinkertainen asia. Järjestelmien testaukseen ei ole olemassa standardoitua tapaa. Kaupallisesti suoritetuista testeistä ei ole tarkkaa tietoa saatavilla [8]. Keskeinen ongelma testaustavoissa on, että kukin organisaatio voi käyttää IDPS-järjestelmää eri tavalla kuin muut. Organisaatioiden olisikin suositeltavaa laatia itse testaussuunnitelma ja sen pohjalta testausprosessi omaan käyttöönsä. Scarfone ym. huomauttavat vielä, että vaikka testaamista olisi hyvä tehdä laboratorio-olosuhteissa, se ei tuota kaikin osin oikeita tuloksia, sillä kaikenlaista tuotantoympäristössä ilmenevää liikennettä on hankala toistaa laboratorio-olosuhteissa [8]. Jokainen ympäristö, jossa IDPS on käytössä, tulisikin siis testata erikseen.

Koska testaamistapoja ei ole standardoitu, ei saatavilla myöskään ole valmiita ohjelmistoja, joilla testaamista voisi suorittaa [8]. Tämän vuoksi organisaation täytyykin itse

ratkaista, miten testaussuunnitelman mukainen testaus toteutetaan. Testauksessa täytyy generoida reaalimaailman potentiaalisia uhkia vastaavaa haittaliikennettä ja hyökkäyksiä. Jotta tämä voidaan tehdä, täytyy uhat ja niiden pohjalta tehtävät hyökkäykset ensin tunnistaa. Scarfone ym. huomauttaa myös, että IDPS:n käyttämiä erilaisia tunnistusmenetelmiä pitäisi testata eri tavalla [8]. Esimerkiksi tunnistepohjainen järjestelmä vaatii erilaiset testit kuin tilallista protokolla-analyysia käyttävä järjestelmä. Aluksi onkin tarpeen selvittää, mitä tunnistusmenetelmiä organisaation valitsema IDSP-tuote käyttää. Tämä ei ole välttämättä aivan selvää, sillä IDPS-tuotteiden valmistajat voivat nimetä tuotteidensa ominaisuuksia hämäävästi. Esimerkiksi Ciscon Deep Packet Inspection on toimintansa puolesta hyvin lähellä tilallista protokolla-analyysia [11].

Testauksen lähtökohtana täytyy pitää organisaation tarpeita. Tällaisia ovat muun muassa tuotteen suorituskyky, käyttö, hallittavuus ja yleisesti ottaen toiminta organisaation toimintaympäristössä. Testauksessa kannattaa myös huomioida muistakin lähteistä, kuten kolmansien osapuolien tekemistä testeistä ja tuotteen valmistajan dokumentaatiosta, saatu tieto. Myös henkilöstön kokemus tuotteista kannattaa ottaa huomioon. Scarfone ym. esittävätkin, että näiden menetelmien avulla organisaatio voi rajata mahdollisten tuotteiden joukkoa pienemmäksi, ja tarvittaessa testata jäljelle jääneitä itse [8]. Tärkeintä testausprosessissa on kuitenkin keskittyä testeihin, joista organisaatio voi saada helpoiten tarkimmat tulokset auttamaan IDPS:n toiminnan arvioinnissa.

# 3. ASIAKASJÄRJESTELMIEN SUOJAAMINEN

Ideaalisesti toimiva IPS estää hyökkäykset ja muun ei-toivottavan liikenteen ja päästää lävitseen kaiken muun. Käytännössä tämä ei kuitenkaan ole mahdollista, sillä jokainen hyökkäyksenestojärjestelmä tuottaa joissakin tilanteissa vääriä positiivisia tai vääriä negatiivisia.IPS-järjestelmän suurimpana käytännön ongelmana voidaankin pitää väärien hälytysten määrää [12]. Asiakkaiden järjestelmiä ja palveluita suojatessa tämä tulee ottaa erityisen hyvin huomioon, sillä väärin perustein estetyn liikenteen vaikutukset voivat näkyä asiakkaan liiketoiminnassa asti. Tämä pätee erityisesti erilaisiin verkkokauppaympäristöihin. Pääsääntönä voidaankin pitää, että jos tietty sääntö voi laukaista väärän hälytyksen, sellaisen ei tulisi automaattisesti laukaista estoa liikenteelle [12]. Käytännössä tätä on kuitenkin vaikea toteuttaa sillä se edellyttäisi jokaisen tunnisteen testaamista monipuolisesti erilaisilla liikennevirroilla.Onkin syytä tiedostaa väärien positiivisten mahdollisuus ja niistä aiheutuvat vaikutukset myös asiakkaiden näkökulmasta.

Tässä luvussa tarkastellaan hyökkäyksenestojärjestelmän ominaisuuksia Ghorbanin ym. kirjassa Network Intrusion Detection and Prevention esittämän jaon mukaan. Samalla käsitellään kyseisten ominaisuuksien tärkeyttä asiakasjärjestelmien kannalta.

## 3.1 Tarkkuus

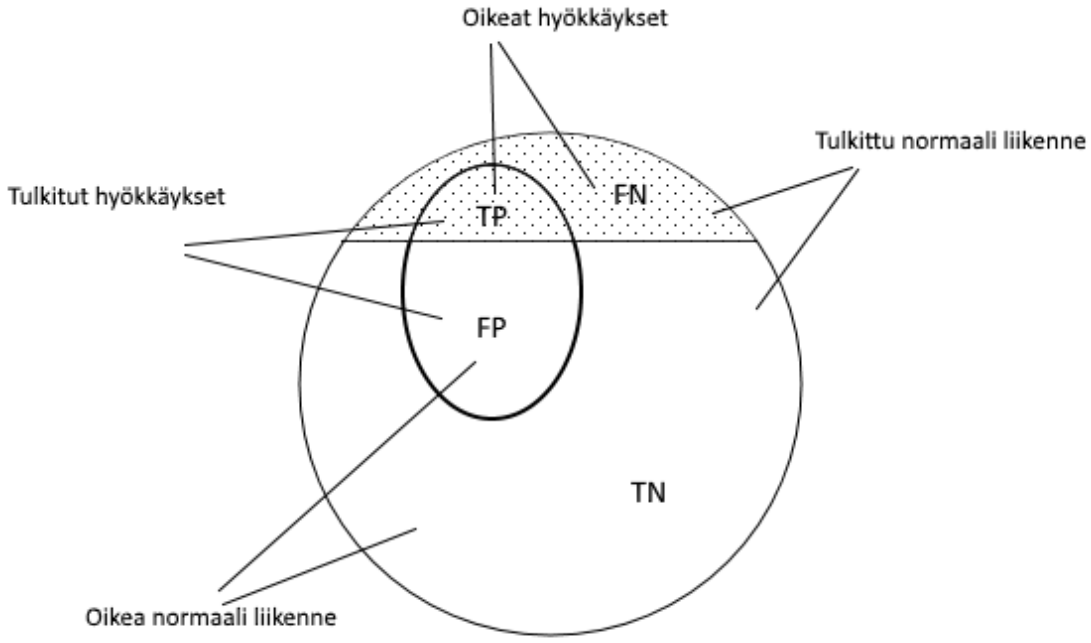
Tarkkuudella tarkoitetaan sitä kuinka tarkasti IDPS-jäjestelmä tunnistaa paketteja oikein. Mittauksen kohteena voivat olla niin järjestelmän läpi päästämien hyökkäysten määrä ja laatu kuin tuotettujen väärien positiivisten määrä[15]. Taulukossa yksi on esitetty mihin tuloksiin IDPS-järjestelmä voi tulla tulkitessaan liikennettä.

| | **Liikenteen tyyppi** | **IDPS:n tulkinta liikenteestä** |
|---|---|---|
| **Oikea positiivinen (TP)** | Hyökkäys | Hyökkäys |
| **Väärä positiivinen (FP)** | Normaali | Hyökkäys |
| **Oikea negatiiinen (TN)** | Normaali | Normaali |
| **Väärä negatiivinen (FN)** | Hyökkäys | Normaali |

***Taulukko 1.*** *IDPS:n liikennetyypit ja tulkinta*

Taulukossa liikenne on jaettu karkeasti normaaliin liikenteeseen ja hyökkäykseen. IDPS voi tulkita normaalin liikenteen joko oikein normaaliksi liikenteeksi tai sitten väärin

hyökkäykseksi. Vastaavasti hyökkäykset voidaan tulkita oikein hyökkäyksiksi tai väärin normaaliksi liikenteeksi.Koukousoulaym. kuvaakin tilannetta kuvan viisi esittämällä tavalla, huomioiden samalla liikennetyyppien ja tulkintojen osuudet kokonaismääristä [16].




***Kuva 5.*** *IDPS:n liikennetyyppien osuudet ja tulkinnat (mukailtu [16]:sta)*

Hyökkäys taas voi tapahtua hyvin monella eri tavalla, joten sen tunnistaminen voi olla vaikeaa. Hyökkäykset voidaan jakaa myös tapahtuvaksi odotetulla tai odottamattomalla tavalla. Odotetut hyökkäykset ovat järjestelmän kannalta helpompia tunnistettavia, koska ne täyttävät tyyppilisien hyökkäyksien tunnusmerkit. Odottamattomia hyökkäyksiä vastaan ei ole olemassa selkeitä tunnusmerkkejä, joten niiltä suojautuminen aiheuttaa vääriä hälytyksiä. [15]

Valtaosa kaikesta liikenteestä on normaalia liikennettä[16]. Testidatalla suoritettu tilastollinen analyysi tukee myös kuvassa viisi esitettyä tilannetta, jonka mukaan valtaosa kaikesta IDPS:n väärin tulkitsemasta liikenteestä on vääriä positiivisia [17]. Asiakasjärjestelmien suojaamisen kannalta onkin tärkeää pohtia, kuinka paljon väärien positiivisten määrää halutaan minimoida. Tämä riippuu paljon suojattavista palveluista, ja esimerkiksi verkkokauppojen kohdalla pelkkä sekunnin viive voi vaikuttaa myyntiin merkittävästi, joten sillä, että IPS estää jonkin sivun latautumisen väärin perustein on varmasti myös vaikutusta [18].Asiakkaan palvelukokemuksen kannalta lienee parempi, että IPS on säädetty siten, että väärät positiiviset pyritään minimoimaan, vaikka se laskee myös oikeiden positiivisten määrää.

## 3.2 Suorituskyky

IDPS-järjestelmän tehokkuuteen vaikuttavat hyvin monet seikat aina käytettävästä fyysisestä laitealustasta alkaen. Tärkein suorituskyvyn mittari on verkkoperusteisen hyökkäyksenestojärjestelmän kyky prosessoida nopeassa verkkoliitännässä kulkevaa liikennettä reaaliaikaisesti ilman merkittävää pakettihävikkiä [15].

Verkkoperusteisen tunnistepohjaisen IDPS:n suorituskyvyn mittaukseen on joitakin menetelmiä. Yksi sellainen on Schaelickenym. esittämä menetelmä [19]. Sen perusperiaatteena on, että jos liikenteen määrän pysyy vakiona, IDPS-järjestelmän suorituskyky riippuu käytetyistä tunnisteista ja järjestelmän prosessointikyvystä. Tunnisteet taas voidaan jakaa karkeasti kahteen ryhmään sen mukaan tarkastelevatko ne paketin otsikkokenttiä vai kuormaa. Otsikkokentän koko ei merkittävästi muutu, joten sitä tarkastelevien sääntöjen aiheuttama kuorma aiheutuu suoraan pakettien määrästä. Kuormaa tarkastelevien sääntöjen osalta tilanne on toinen, koska pakettien koko voi todellisessa liikenteessä vaihdella. Tästä syystä pakettien koko vaikuttaa niiden lukumäärää enemmän järjestelmän suorituskykyyn. [19]

Kun IDPS:lle ohjatun liikenteen määrä ylittää sen prosessointikyvyn, se pudottaa paketit, joita se ei pysty prosessoimaan [19]. Suoraan liikennevirtaan sijoitetuissa järjestelmissä tämä siis estää suojatun palvelun käytön kokonaan. IPS:n prosessointikyky on todennäköisesti suojattavien asiakasjärjestelmien määrää eniten rajaava tekijä, joten siihen on syytä kiinnittää huomiota järjestelmää valitessa. Yksittäisen tunnisteen vaikutus prosessointikykyyn on kuitenkin pieni, ja ainoastaansen perusteella ei kannata lähteä ottamaan tiettyjä tunnisteita pois käytöstä.

## 3.3 Kokonaisvaltaisuus

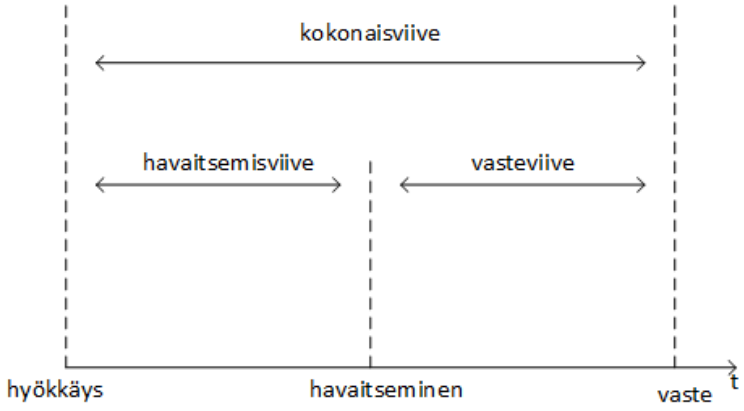
Kokonaisvaltaisuudella tarkoitetaan IDPS-järjestelmän kattavuutta erilaisten uhkien suhteen. Tätä ei ole mahdollista mitata tarkkaan, koska täysin ajantasaista listaa kaikista hyökkäyksistä ei voi olla olemassa. IDPS-järjestelmältä tulisi kuitenkin edellyttää suojausta kaikkia tunnettuja haavoittuvuuksia vastaan. Tämän lisäksi järjestelmän pitäisi pystyä reagoimaan myös tuntemattomiin uhkiin, jonkinlaisen heuristiikan avulla. [15]

Kaupallisten IDPS-järjestelmien kanssa on syytä huomioida tunnistepäivitysten nopeus. Uusia haavoittuvuuksia ilmenee kuitenkin jatkuvasti, ja niitä pystytään hyödyntämään tuntien sisällä havaitsemisesta, minkä vuoksi on tärkeää, että tunnisteet päivittyisivät nopeasti. Eri IPS-tuotteiden valmistajat lupaavat tunnistepäivityksiä yleensä tuntien tai päivien sisään haavoittuvuuden kriittisyydestä riippuen. Esimerkiksi Cisco julkaisee uusia tunnistepäivityksiä yleensä kerran viikossa, mutta kriittisempiin haavoittuvuuksiin pyritään reagoimaan tunneissa [20].

Asiakasjärjestelmien suojauksen kannalta mahdollisimman kattavat tunnisteet antavat tietysti asiakkaalle kattavampaa suojaa, mutta täydellinen suojaus ei koskaan ole. Tunnistepäivitykset kannattaa hankkia luotettavasta lähteestä, jotta niihin voidaan luottaa, ja ne saadaan mahdollisimman vähällä työllä IPS:n käyttöön.

## 3.4 Vasteen nopeus

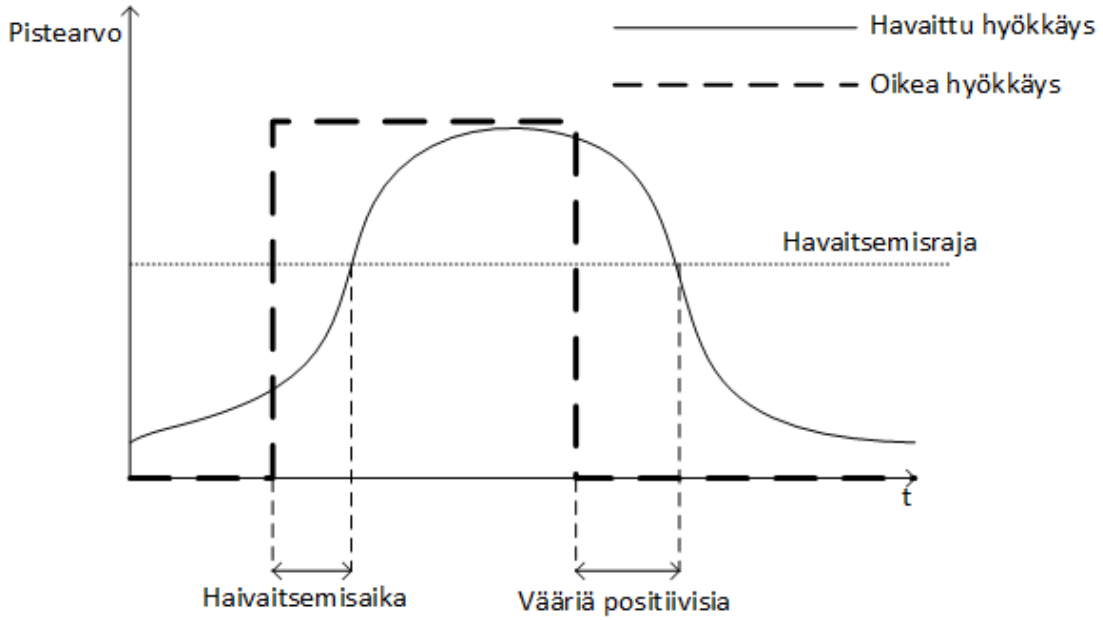
Hyökkäyksen käynnistymisen jälkeen IDPS-järjestelmältä menee ensin aikaa hyökkäyksen havaitsemiseen. Sen jälkeen kuluu aikaa ennen kuin järjestelmä reagoi havaittuun hyökkäykseen. Ghorbani ym. kuvaavat tilannetta kuvassa kuusi kuvatulla tavalla.




***Kuva 6.*** *Viiveet IDPS:n toiminnassa (mukailtu [15]:sta)*

Molemmat viiveet vaikuttavat järjestelmän toimintaan.Vasteviiveeseen on helpompi vaikuttaa, sillä hyökkäyksen havaitsemiseen ja tunnistamiseen tulee aina menemään aikaa [15]. Reaaliaikaisessa IDPS-järjestelmässä havaitsemisviive on nykyään käytännössä nolla, tai ainakin hyvin lähellä sitä. Jos tilannetta verrataan ensimmäisiin IDS-järjestelmiin, joissa hyökkäykset havaittiin järjestelmänvalvojan käydessä lokeja läpi, on kehitys mennyt merkittävästi eteenpäin.

IDPS-järjestelmän vasteen nopeuden arviointiin on olemassa joitakin menetelmiä, joista Dokas ym. esittelee kaksi. Nämä ovat purskeen havaitsemistaso (burst detection rate) ja havaitsemisaika (detection time)[21]. Menetelmiä on kuvattu kuvassa seitsemän.




***Kuva 7.*** *IDPS:n vasteaika ja hyökkäysten pisteytys (mukailtu [21]:sta)*

Kuvassa vaaka-akselilla kuvataan aikaa ja IDPS:n keräämän datan pistearvoa. Pistearvo kuvaa todennäköisyyttä, että IDPS:n tietyllä hetkellä käsittelemä data on hyökkäys. Kun pistearvo ylittää tietyn havaitsemisrajan, IDPS tulkitsee hyökkäyksen käynnistyneen. Tämän ajanhetken ja hyökkäyksen oikean käynnistymishetken välinen aika on havaitsemisaika.Purskeen havaitsemistasolla taas tarkoitetaan hyökkäyksen sitä osaa, jolloin hyökkäys on käynnissä ja IDPS-järjestelmä on tunnistanut sen oikein hyökkäykseksi. Kuvasta viisi tämä voidaan nähdä välinä, jolloin havaittu hyökkäyskäyrä leikkaa havaitsemisrajan ja oikea hyökkäyskäyrä leikkaa havaitsemisrajan toiseen kertaan.

Suoraan liikennevirtaan sijoitetun IDPS:n vasteaikavaatimukset ovat kovemmat kuin liikennevirran rinnalle sijoitetun. Liikenteen määrien kasvaessa liikennevirran rinnalla oleva IDPS ainoastaan jättää paketteja käsittelemättä, ja voi pahimmassa tapauksessa päästää hyökkäyksen läpi tai havaita sen liian myöhään. Liikennevirrassa oleva IDPS voi ruuhkautuessaan estää hyväksytyn normaalin liikenteen läpipääsyn. [15]

Käytännössä IDPS-järjestelmän kokonaisviivettä on vaikea määrittää. Kontrolloidussa ympäristössä, jossa hyökkäyksen todellinen aloitushetki on tiedossa, havaitsemisaika ja vasteaika ovat kuitenkin laskettavissa. [15]

Vasteen nopeus ei suoranaisesti vaikuta asiakasjärjestelmien suojaamiseen. Siihen ei ole käytännössä mahdollistavaikuttaa enää järjestelmän valinnan jälkeen.Mikäli vasteen nopeuden suhteen on vaatimuksia, ne tulee huomioida käytettävää järjestelmää valitessa.

## 3.5 Mukautuvuus ja kustannustehokkuus

Koska reaalimaailman IDPS-järjestelmän käytettävissä olevat resurssit ovat rajalliset, ei kaikkiin havaittuihin hyökkäyksiin ole välttämättä mielekästä reagoida, eikä kaikkia uhkia kannata edes yrittää havaita. Jos hyökkäys vaatii IDSP-järjestelmältä merkittävää prosessointia, mutta on vaikutuksiltaan vähäinen, voidaan kyseiset hyökkäykset ohittaa kokonaan IDPS-järjestelmässä. Tällöin järjestelmän resurssit vapautuvat muunlaisten uhkien havainnointiin ja prosessointiin. Voidaan sanoa, että kustannustehokas IDPS-järjestelmä osaa tasapainottaahyökkäysten aiheuttamat vahingot ja järjestelmän tekemien vastatoimien hinnat.Se osaa tämän perusteella ratkaista, mihin tilanteisiin reagoidaan estotoimilla[22]. Esimerkiksi porttiskannaus voidaan jättää havaitsematta, sillä vaikka se on IDPS:n näkökulmasta helppo havaita, se ei aiheuta suoranaista vahinkoa[22].

Lee ym. esittävät mallin hyökkäysten kustannusten määrittelyyn hyökkäyksen havaitsemisen ja toteutettavan vasteen näkökulmasta [23]. Malli määrittelee neljä eri kustannusta:

- Vahingon kustannus (Damage Cost, DC): Kohderesurssiin aiheutuneen vahingon määrä, kun IDPS ei reagoi hyökkäykseen.
- Vasteen kustannus (Response Cost, RC): Hyökkäykseen vastaamisen hinta. Ottaa huomioon myös vasteesta aiheutuvat muuta liikennettä mahdollisesta haittaavat vaikutukset.
- Toiminnaliset kustannukset (Operational Cost, OC): Liikenteen analysoinnista ja muut IDPS:n toimintaan liittyvät kustannukset mukaan lukien järjestelmän ylläpidon ja suunnittelusta aiheutuvat kustannukset.
- Johdettu kustannus (Consequential Cost, CC): Kuvaa hyökkäyksen havainnoinnin lopputulosta. Esim. oikea negatiivinen, väärä negatiivinen, oikea positiivinen, väärä positiivinen.

Hyökkäyksen havaitseminen ei ole hyödyllistä, jos siitä aiheutuvat toiminnalliset kustannukset ovat suuremmat kuin hyökkäyksen aiheuttama vahinko. Mukautuva, kustannustehokas IDPS-järjestelmä ottaa tällaiset näkökulmat huomioon arvioidessaan vastetta havaittuun hyökkäykseen. IDPS muodostaa hyökkäyksen havaittuaan varmuusluvun, joka kuvaa todennäköisyyttä, jolla havaittu hyökkäys on oikea. Vastatoimet voidaan käynnistää ainoastaan, jos varmuusluku on riittävän suuri. Tämä ei vielä yksistään riitä, vaan järjestelmän tulee vielä arvioida, onko vahingon kustannus riittävän suuri verrattuna muihin kustannuksiin. [23]

Väärän negatiivisen tapauksessa (FN) IDPS on päästänyt läpi hyökkäyksen reagoimatta siihen. Tällöin hyökkäyksen johdettu kustannus on yhtä kuin vahingon kustannus. Oikean negatiivisen tapauksessa(TN) CC on määritelty nollaksi. IDPS:n määritellessä normaalin tapahtuman hyökkäykseksi (FP), johdetuksi kustannukseksi tulee vasteen kustannus. On tietenkin mahdollista, että hyökkäyksen varmuusluku ei ylitä vasteeseen vaadittavaa tasoa, jolloin johdettu kustannus on nolla. Neljännessä tapauksessa IDPS tunnistaa hyökkäyksen oikein (TP). Tällöin CC on yhtä kuin vasteen kustannus. On kuitenkin mahdollista, että järjestelmässä olevien viiveiden vuoksi hyökkäys on jo ehtinyt aiheuttaa vahinkoa, jolloin CC on suurempi kuin vasteen kustannus. [23]

Tämä malli soveltuu hyvin käytettävien tunnisteiden valintaan myös asiakasjärjestelmiä suojatessa. Ennen eri kustannusten laskemista, täytyy pystyä tunnistamaan asiakasjärjestelmien kannalta kriittisimmät haavoittuvuudet eli ne, joissa on suurin vahingon kustannus. Vahingon kustannuksista ja niihin liittyvistä johdetuista kustannuksista saadaan hyvä lähtökohta IPS:n sääntöjen optimointiin.

## 3.6 Hyökkäyksenkestokyky

Ensimmäisen sukupolven IDS-järjestelmät olivat paljolti päätelaiteperustaisia ja valvoivat vain samaa kohdetta, jolle ne olivat asennettuna. Tämä aiheutti ongelman, sillä tunkeutuja pystyi helposti sammuttamaan IDS:n päästyään järjestelmään varsinkin,koska järjestelmä ei välttämättä hälyttänyt automaattisesti tunkeutumisesta. Päätelaiteperusteisia järjestelmiä on edelleen käytössä, ja ne ovat edelleen haavoittuvia, jos tunkeutuja saa pääsyn samalla laitteelle. [15]

Verkkoperusteiset IDPS-järjestelmät eriyttävät tunkeutumisen havaitsemisen eri laitteelle kuin hyökkäyksen kohde, joten ne eivät itsessään vaarannu hyökkäyksen tapahtuessa. Tämä ei sinällään estä IDPS:n joutumista hyökkäyksen kohteeksi, mutta hyökkääjään pitää nähdä lisävaivaa koska hyökkäyskohteita on yhden sijasta kaksi.

Yleensä IDPS-järjestelmissä jokainen komponentti on keskitetty ja siten jokainen niistä voi hajotessaan aiheuttaa järjestelmän lamaantumisen. Yksittäisen komponentin hajoaminen voi aiheutua esimerkiksi DOS-hyökkäyksestä, tietoliikenneyhteyksien ongelmista tai hyökkääjän syöttämästä väärästä datasta. Verkkoperusteisia järjestelmiä voi myös olla mahdollista kiertää tai niihin voidaan syöttää väärää dataa. [15]

IDPS-järjestelmän pitäisi pystyä toimimaan riippumatta käynnissä olevista hyökkäyksistä. Niiden pitää pystyä käsittelemään läpikulkevaa liikennettä ilman merkittävää vaikutusta IDPS:n suojaamiin palveluihin. Näiden vaatimusten täyttämiseksi IDPS-järjestelmissä käytetään tiettyjä tekniikoita järjestelmän suunnitteluun ja toimintaan liittyen.

# 4. IPS-TUOTTEIDEN MARKKINAKATSAUS

Tässä luvussa käsitellään sitä, mitä IPS-palveluun voi sisältyä, millaisia ominaisuuksia siltä voi odottaa, mitä rajoituksia tekniikka asettaa tarjottavalle tuotteelle ja millaisia tuotteita on jo nyt tarjolla. Kantaa otetaan myös palveluntarjoajaan kohdistuviin vaatimuksiin ja siihen, millaiset tahot voisivat toimia palveluntarjoajina.

Tässä kohtaa on myös tarpeen tehdä ero IPS-ratkaisun ja IPS-palvelun välillä. Palveluntarjoaja tuottaa IPS-ratkaisun avulla asiakkaalle tarjottavan IPS-palvelun. IPS-palvelun voidaan siis katsoa koostuvan sopivasta IPS-ratkaisusta ja palveluntarjoajan osaamisesta sen hallinnassa.

## 4.1 Kuka voi tarjota IPS-palvelua

IPS-palvelun täytyy verkkotopologian näkökulmasta sijaita suojattavan palvelun tai verkon ja sen käyttäjien ja oletettujen hyökkääjien välissä. Tällöin tämän kaltaista palvelua pystyvät parhaiten tarjoamaan toimijat, jotka jo muutoinkin sijaitsevat sopivassa kohtaa verkkotopologiaa. Tällaisia tahoja ovat siis asiakkaan Internet-palveluntarjoaja, erilaiset CDN-palveluita (Content Delivery Network) tarjoavat tahot tai asiakkaan palveluita tai palvelimia ylläpitävät tahot.

## 4.2 IPS-palvelun kohderyhmät

IPS-palveluiden tuotteistuksesta puhuttaessa täytyy ensin tehdä jako kuluttajille ja yrityksille suunniteltujen tuotteiden välillä. Kuluttajille suunnatut ratkaisut ovat yleensä enemmän erilaisia palomuuri- ja virustorjuntaratkaisuita, joissa voi kuitenkin olla mukana IPS:n kaltaista toiminnallisuutta, kuten esimerkiksi Elisan tarjoama Tietoturvapaketti, joka suorittaa jonkinlaista reaaliaikaista liikenteen tarkastelua [24].

Yrityksille suunnatut tuotteet voivat olla hyvin monipuolisia, ja sisältää vain IPS:n tietyn toiminnallisuuden. Esimerkiksi Elisa on luonut yrityksille suunnatun Elisa Kilpi -palvelun, jolla voi torjua erilaisia DoS-hyökkäyksiä [25]. Tästä erillään tarjotaan kuitenkin Elisa Palomuuripalvelua, joka kuitenkin kuvauksensa perusteella käyttää automaattisesti pilvestä päivittyviä haittaohjelmatunnisteita, mikä taas viittaa enemmän IPS-järjestelmän kuin varsinaisen palomuurin toiminnallisuuteen [26].

## 4.3 Markkinoilla olevia IPS-tuotteita

Monet Internet-palveluntarjoajat ja CDN-toimittajat tarjoavat kukin omanlaisiaan IPS-tuotteita. Tällaisia ovat mm. luvussa 4.2-mainitut Elisa Kilpi ja Elisa Palomuuripalvelu. Tuotteen kuvauksesta ei käy ilmi, millaisilla ratkaisuilla mainittuja palveluita tarjotaan, mutta palvelun ominaisuudet viittaavat uuden sukupolven palomuuriin. Myös muilla suomalaisilla Internet-palveluntarjoajilla on vastaavanlaisia tuotteita, kuten esimerkiksi Sonera Verkkosuoja ja Sonera Palomuuri [27][28]. Näistä Verkkosuoja on Soneran vastine Elisa Kilpi-palvelulle, eli sen tarkoitus on siis suojata palvelua palvelunestohyökkäyksiltä. Sonera Palomuuri on taas Elisan tuotetta monipuolisempi, sillä sitä tarjotaan sekä asiakaskohtaisena että verkkopohjaisena [28].

CDN-tarjoajien IPS:n kaltaiset palvelut vaihtelevat paljon tarjoajan mukaan. Tarjolla on Akamain tarjoaman Kona Site Defenderin kaltaisia kokonaisvaltaisempia tuotteita, jotka torjuvat DoS-hyökkäysten lisäksi myös sovellustason hyökkäyksiä, kuten SQL-injektioita tai HTTP-protokollan sisältä tapahtuvia hyökkäyksiä [29]. Toisaalta Cloudflare puolestaan tarjoaa ilmaisella perustason asiakkuudellaan suojaa DoS hyökkäyksiä vastaan, mutta muunlaiseen tarkempaan liikenteen suodatukseen perustuvasta turvasta täytyy sitten maksaa [30]. CDN tarjoajien tuotteita yhdistää usein mahdollisuus suodattaa palvelun liikennettä lähdeosoitteen maineen mukaan [30][31].

Yleisesti ottaen CDN-tarjoajat markkinoivat palveluitaan tehokkaammin kuin ISP:t. ISP ei tietenkään voi tarjota palveluaan kuin omille asiakkailleen, joten niiden potentiaalinen asiakaskunta on pienempi kuin CDN-tarjoajilla. Yleistä tuntuukin olevan, että CDN-tarjojat markkinoivat palveluitaan pakettina, jolla verkkopalvelun saa kerralla turvalliseksi ja suorituskykyiseksi [32].

Asiakkaan näkökulmasta Internet-palveluntarjoaja tai palveluita ylläpitävä taho voi olla kuitenkin CDN-tarjoajaa houkuttelevampi IPS-toimittaja. Mikäli asiakas ei ole kiinnostunut varsinaisesta CDN-palvelusta vaan haluaa vain lisätä palvelunsa turvallisuutta, on CDN-toimittaja vain ylimääräinen osapuoli, mikäli ISP tai palvelua ylläpitävä taho tarjoavat myös IPS-palvelua. On myös huomionarvoista, että kaikilla CDN-tarjoajilla ei ole omaa sisällönjakopalvelinta Suomessa, jolloin suorituskyky CDN:n kautta voi olla huonompi kuin ilman.

## 4.4 IPS-tuotteen rajoitteet

IPS-palveluun kohdistuu sen tarjoajan näkökulmasta teknisiä ja muita rajoitteita. Kysymys on rajallisesta resurssista, joka pitäisi jakaa asiakkaiden kesken kilpailukykyiseen hintaan, mutta kuitenkin omat kulut kattaen. Rajoitteita tuotteelle asettavat lähinnä käytettävän laitteistoin prosessointikyky ja erilaiset, lainsäädännöstä, asiakkailta, standardeista, ja valituista teknologioista tulevat vaatimukset.

### 4.4.1 Laitteiden prosessointikyky

IDPS-laitteiden suorituskykyä mitataan laitteen kyvyllä prosessoida liikennettä tiettyä aikayksikköä kohden. Pienimmät IDPS-laitteet prosessoivat yleensä noin 200Mbps ja suurimmat pääsevät taas kymmeniin gigabitteihin per sekunti. Käytännössä pienemmät laitteet soveltuvat pienien yritysten tarpeisiin, jos tarvitaan laite suojaamaan kaikkea yrityksen verkkoliikennettä. Pienempiä laitteita voidaan käyttää myös suuremmissa yrityksissä, mutta tällöin syytä miettiä tarkemmin, mikä kaikki liikenne kuljetetaan IPS:n läpi.

### 4.4.2 Muut tekniset rajoitteet

On huomionarvoista, että IDPS-laitteet eivät pysty purkamaan salattua liikennettä. Tällöin esimerkiksi SSL-suojattua palvelua koskevaa liikennettä ei pystytä suodattamaan. Mikäli liikenne kuitenkin halutaan prosessoida IDPS:llä, täytyy SSL-suojaus purkaa liikenteestä ennen suodatusta. Käytännössä tämä tarkoittaa erillisen SSL-välityspalvelimen käyttöä, joss suojaus puretaan ja liikenne ohjataan IDPS:lle, minkä jälkeen liikenne on mahdollista tarvittaessa salata uudelleen. Tällöin IDPS-toimittajalla täytyy olla käytetyn SSL-sertifikaatin avainosa.

### 4.4.3 Ulkoiset rajoitteet ja vaatimukset

Joidenkin tietoturvastandardien ja -kriteeristöjen vaatimukset edellyttävät myös IDPS-järjestelmien käyttöä. Suomessa näistä merkittävin on kansallinen turvallisuus- ja auditointikriteeristö, eli Katakri. Katakri ei itsessään ole tietoturvastandardi, vaan se perustuu Suomen voimassa olevaan lainsäädäntöön ja kansainvälisiin tietoturvavelvoitteisiin. Katakrin vaatimukset täyttämällä, yrityksen toiminta täyttää Suomen lainsäädännön vaatimusten lisäksi myös Suomea sitovat kansainväliset velvoitteet. Tämä kattaa myös EU:n asettamat veloitteet. [33]

IDPS-järjestelmien näkökulmasta kiinnostava kohta Katakrissa on I-osan kohta 1, jossa korostetaan poikkeamien havainnointia ja keinoja estää ja rajata hyökkäykset tietojenkäsittely-ympäristöä vastaan [33].

Toinen IDPS-järjestelmien käyttöä edellyttävä dokumentti on PCI-DSS(Payment Card Industry Data Security Standard)-standardi. Standardin täyttäminen on edellytys korttimaksamiseen liittyvien tietojen tallentamiseen, käsittelyyn ja siirtämiseen. [4]

PCI-DSS:n kohta 11.4.edellyttää IDS- tai IPS-järjestelmän käyttöä hyökkäyksien estoon ja havainnointiin korttimaksamiseen liittyvien järjestelmien kanssa [4]. Standardi ottaa myös tarkasti kantaa siihen, miten IDPS-järjestelmän tulee hälyttää asianomaisia poikkeuksen havaittuaan, ja että sen tunnistepäivitysten tulee olla ajantasalla. [4]

## 4.5 Tuotteiden hinnoittelu

Olemassa olevat IDPS-tuotteet ovat pääosin kiinteällä kuukausimaksulla toimivia, tiettyyn IDPS:n ominaisuuteen tai ominaisuusjoukkoon keskittyviä kokonaisuuksia. Erilaisia lisäpalveluita ja korotettua vastetta on tarjolla lisähintaa vastaan.

Soneran Palomuuri-palvelun tapauksessa hintaan vaikuttava suojattavan yhteyden nopeus, eli käytännössä datamäärä aika yksikköä kohden, haluttu palvelutaso ja mahdolliset lisäpalvelut, kuten asiakkaalle mahdollisuus seurata järjestelmän lokeja tai muuta asiakaskohtaista kustomointia. Tämän kokonaisuuden hinnat ovat alkaen 59 euroa kuukaudessa, ja voivat suojattavan liikennemäärän ja haluttujen lisäpalveluiden mukana nousta aina yli 1500 euron. Elisan vastaavankaltaisesta Palomuuripalvelusta ei löydy hintatietoja suoraan verkosta.

DoS-hyökkäysturvaa tarjotaan halvimmillaan ilmaiseksi esimerkiksi Cloudflaren taholta [30]. Maksamalla on kuitenkin mahdollista hankkia korkeamman tasoista palvelua, joilla mukaan saa parempaa DoS-turvaa, ja sivustokohtaista liikenteen suodatusta ja uhkien torjuntaa. Näiden myötä palvelun hinta kohoaakin sitten 200$:iinyhtä suojattua sivustoa kohden [30]. Datamäärärajoituksia ei Cloudflarella ole [30]. Akamain Kona Site Defenderin tai kotimaisten operaattorien DoS-suojaukseen tarkoitettujen palveluiden hintoja ei ollut verkossa nähtävillä.

Yleisesti ottaen tuotteissa ei ole keskitytty niinkään oikeasti prosessoitavaan datamäärään, vaan annetaan asiakkaan arvioida itse, millaisen palvelun tahtoo, ja laskutetaan valitun palvelun mukaan. Rajallisin resurssi vaikuttaa selkeästi myytäviin tuotteisiin, sillä esimerkiksi CDN-tarjoaja Cloudflare ei veloita asiakkaita käytetyn kaistan mukaan, kun taas esimerkiksi Soneralla se on palvelun hintaan suurin yksittäinen vaikuttava tekijä. Näin ollen palvelun hintataso voi riippua hyvin paljon tarjoajan sijainnista asiakkaan verkkotopologiassa.

# 5. IPS-JÄRJESTELMÄN TUOTTEISTUS

Hyökkäyksenestojärjestelmää haluttiin käyttää asiakasjärjestelmien suojaamisen, ja siten tuotteistaa sen toiminta. Pohjimmiltaan kyse on asiakkaan palvelimeen tai palveluun kohdistuvan liikenteen ohjaamisesta IPS-laiteelle, mutta varsinaiseen tuotteeseen voi liittyä paljon muutakin. Luotava tuote on tässä tapauksessa IPS-palvelu, joka toteutetaan jollakin olemassa olevalla IPS-teknologialla. Tuotteella pyritään suojaamaan yrityksen omassa konesalissa ajettavia asiakkaiden palveluita ja palvelimia. Käytännössä tämä tarkoittaa jonkin markkinoilla olevan IPS-teknologiaa käyttävän IPS-laitteen hankintaa, konfigurointia ja muiden palvelun elinkaareen kuuluvien seikkojen suunnittelua.

Tuotteistus jakautuu tämän dokumentin puitteissa neljään vaiheeseen. Suunnittelu- ja markkinointivaihe käsittelee, millaiseen tarpeeseen luotava tuote vastaa, kenelle ja minkälaisilla asioilla sitä voidaan markkinoida. Samalla käsitellään myös millaisia vaatimuksia nämä asettavat tuotteistettavalle IPS-teknologialle.

Toteutusvaiheessa käsitellään sopivan IPS-teknologian valintaa ja sen konfigurointia. Tunnisteiden muokkaaminen, ja tunnistejoukkojen luominen ovat keskeinen osa tätä vaihetta. Näiden lisäksi käsitellään myös, miten suunnitteluvaiheessa ideoituja ominaisuuksia voidaan toteuttaa.

Toteutuksen jälkeen siirrytään ylläpitovaiheeseen. Siinä yhteydessä esitellään henkilöstön osaamiseen kohdistuvia vaatimuksia, ja miten vaatimukset voidaan täyttää. Samalla otetaan kantaa myös jokapäiväiseen toimintaan järjestelmän kanssa, ja kuvataan millä tavoin järjestelmän toimintaa valvotaan ja päivitykset muutoksia hallitaan.

Lopuksi käydään läpi tuotteen hallintaanliittyviä seikkoja, kuten tuotteen suorituskyvyn mittaus ja valitun ratkaisun kanssa havaitut ongelmat. Näiden lisäksi pohditaan tuotteen jatkuvuutta, ja tulevaisuuden kehitystä.

## 5.1 Suunnittelu ja markkinointi

Suunnittelu- ja markkinointivaiheessa käydään läpimillaiseen tarpeeseen tuotteella ollaan vastaamassa, ketkä sen potentiaalisia asiakkaita ovat, ja millaisia vaatimuksia tästä aiheutuu valittavaan IPS-teknologiaan. Aluksi käsitellään tuotteen kohderyhmää ja millaisiin tarpeisiin tuotteella halutaan vastata. Luvussa 5.1.2 kuvataan tuotteen toteuttavaan IPS-teknologiaan kohdistuvia vaatimuksia. Varsinaiseen teknologia- tai laitevalintaan ei tässä kohtaa vielä oteta kantaa, vaan se käsitellään luvussa 5.2.1. Luku 5.1.3 käsittelee IPS-teknologiasta aiheutuvia kustannuksia, ja millaista hyötyä kustannuksia

vastaan saadaan. Lopuksi käydään läpi tuotteeseen ideoituja ominaisuuksia, jotka valitulla IPS-teknologialla olisi hyvä pystyä toteuttamaan.

Suunnittelun keskeisenä lähtökohtana on kartoittaa, millaiseen tarpeeseen tuotteella on tarkoitus vastata ja mitä vaatimuksia se asettaa tuotteistettavalle IPS-laitteelle. Aluksi käsitellään suunnittelun lähtökohtia, ja määritellään kenelle tuotetta ollaan tarjoamassa, ja mitä kuluja tuotteen tarjoamisesta aiheutuu. Luvussa 5.1.2 kuvataan IPS-laitteeseen kohdistuvia vaatimuksia, ja miten ne rajaavat sopivan laitteen valintaa. Tuotteeseen ideoituja ominaisuuksia, joilla voidaan tarjota lisäarvoa asiakkaalle, käsitellään luvussa 5.1.3.

### 5.1.1 Tuotteen kohderyhmät

Tuotteen kohderyhmäon tässä tapauksessa asiakkaat, jotka jo ostavat käyttöpalveluita tai tulevat ostamaan sitä tulevaisuudessa. IPS-palvelua tarjotaan siis käyttöpalvelun lisäpalveluna. Kaikki käyttöpalveluita ostavat asiakkaat eivät todennäköisesti ole kiinnostuneita IPS-palvelusta, mutta osaan kohdistuu erilaisia velvoitteita, joihin IPS:llä voidaan vastata. Erilaisten sovelluskehitystyökalujen suhteen sovelluskomponentit, lähdekoodi ja muu tieto itsessään voi olla riittävän arvokasta, jotta sen suojaaminen IPS:llä kannattaa. Julkishallinnon tahot ja muut voittoa tavoittelemattomat organisaatiot voivat puolestaan olla kiinnostuneempia julkisuuskuvansa suojaamisesta. Verkkokauppaympäristöihin kohdistuvat hyökkäykset voivat vaikuttaa kaupassa tapahtuvaan myyntiin, ja sillä tavoin aiheuttaa asiakkaalle taloudellisia tappioita. Verkkokauppoihin liittyy läheisesti myös luottokorttidata, jota käsitellessä PCI-DCC-standardi käytännössä edellyttää IPS-järjestelmän käyttöä [4]. Eri asiakasryhmillä vois siis olla toisistaan eriäviä tavoitteita IPS:llä tavoiteltavista hyödyistä.Valitun IPS-teknologian on pystyttävä palvelemaan näitä kaikkia riittävän monipuolisesti.

### 5.1.2 Vaatimukset IPS-teknologialle

Nykyiset IPS-järjestelmät pystyvät prosessoimaan jopa kymmeniä gigabittejä sekunnissa [34]. Tällaiset laitteet maksavat kymmeniä tuhansia euroja, ja lisäksitulevat yleensä vielä lisenssikulut, joten käyttökustannukset voivat olla todella suuret. Ennen laitteen valintaa onkin hyvä kartoittaa olemassa olevien asiakkaiden kiinnostusta palvelua kohtaan. Hankittavan laitteen prosessointikyky kannattaa mitoittaa ylläpidettäviin palveluihin kohdistuvan liikennemäärän mukaan. IPS:n on pystyttävä prosessoimaan palveluihin keskimäärin kohdistuva liikennemäärä. Liikennemäärän piikkeihin varautuminen on asia, joka on syytä miettiä tapauskohtaisesti. Teoriassa mihin tahansa palveluun voi hetkellisesti kohdistua niin suuri määrä liikennettä, että IPS ei pysty sitä prosessoimaan. Teknologialla asiaa on siis vaikea ratkaista, joten liikenteen maksimimäärä on parempi huomioida esimerkiksi sopimusehdoissa.

Järjestelmän tulee myös olla verkkoperustainen. Tällöin järjestelmän käyttöönotto ei aiheuta muutoksia kohdepalvelimilla tai -palveluissa. Hyökkäyksen ilmetessä IPS-järjestelmä itsessään ei vaarannu ja IPS:n tekemä liikenteen prosessointi ei vaikuta suojattavan kohteen suorituskykyyn.

Järjestelmään täytyy tulla tunnistepäivityksiä riittävän usein ja automaattisesti. Automaation lisääminen lisää järjestelmän hallittavuutta ja vähentää hallinnointiin kohdistuvaa työkuormaa. Automaattisten päivitysten ongelma ovat niissä esiintyvät mahdolliset inhimilliset virheet, jotka voivat aiheuttaa niiden väärän toiminnan. Tästä syystä tunnisteiden tulisikin tulla riittävän luotettavalta taholta, jotta niihin ei päivittäisessä ylläpitotyössä tarvitse puuttua.

### 5.1.3 IPS-teknologian kustannukset

Tuotteen tulee olla taloudellisesti kannattava sitä tarjoavalle yritykselle. IPS-teknologiasta aiheutuu yritykselle hankintakulujen lisäksi käyttöönotto-, ylläpito- ja lisenssikuluja. Hankintakulut kertakustannuksena eivät vaikuta pitkän aikavälin kannattavuuteen, ja myös käyttöönottoon liittyvät kulut ovat kertaluontoisia. Ylläpito sen sijaan on kuluna jatkuva ja siksi IPS-palvelun vaatimaa jatkuvan ylläpidon määrää tulisi minimoida. Tämä onnistuu helpoiten automaatiota lisäämällä ja järjestelmän oikealla konfiguraatiolla. Tähän auttaa myös IPS-teknologian valmistajan tuki, jonka avulla kohdatut ongelmat voidaan selvittää ilman yrityksen sisäistä ylläpitotyötä. Tämän vuoksi erilaisiin tuettomiin tai avoimeen lähdekoodiin perustuviin IPS-teknologioihin perustuvien tuotteiden luomista kannattaa harkita tarkkaan. Teknologian käytöstä aiheutuvien ongelmien selvittelyyn voi kulua odottamattoman paljon aikaa, ja automaattisten tunnistepäivitysten saatavuutta ja luotettavuutta ei voida taata. Kaupallisiin IPS-teknologioihin taas liittyy yleensä hankintakustannusten lisäksi lisenssikustannuksia, mutta niiden vastineeksi saadaan valmistajan tukema teknologia ja tunnistepäivitykset.

### 5.1.4 Tuotteeseen ideoidut ominaisuudet

Hyökkäyksenestojärjestelmän perustoiminnallisuus on estää haittaliikennettä pääsemästä kohdepalveluun. Perustuotetta on hyvä pystyä muokkaamaan asiakkaan toiveiden mukaisesti, jotta palvelulla voidaan paremmin vastata asiakkaan tarpeeseen. Tässä luvussa on esitelty neljä tällaista muokattavaa ominaisuutta, joita tuotteessa voi olla.

Perustilassaan käyttöön valittavan IPS-teknologian toiminta käyttää valmistajan tarjoamaa ja päivittämää tunnistejoukkoja, tai erilaisia poikkeamien havainnointiin perustuvia tunnistusmenetelmiä. Voi kuitenkin olla tilanteita, joissa haluttaisiin käyttää esimerkiksi vain osaa tarjotuista tunnisteista, ja suojata esimerkiksi vain tiettyyn sovellukseen kohdistuvat uhat tai suodattaa ainoastaan haitallisten bottien liikenne. Tällaisia tilanteita varten tuotteen tulisi tarjota mahdollisuus käyttää asiakaskohtaisia tunnistejoukkoja.

Valmistajan tarjoama tunnistejoukko ei välttämättä kata kaikkia uhkia joita asiakkaan järjestelmiin kohdistuu. Tarvitaan muokattuja tunnisteita, jotta tietty uhka voidaan torjua. Tunnisteiden luominen pitäisi tosin aina olla vain toissijainen keino haavoittuvuudelta suojautumiseen.Lähtökohtaisesti pitäisi pyrkiä haavoittuvan sovelluksen korjaamiseen.

Asiakkaalle on kyettävä toimittamaan raportteja IPS-palvelun toiminnasta, ja sen havaitsemista ja estämistä tapahtumista. Niiden avulla asiakkaalle on helppo osoittaa palvelusta saadut hyödyt. Raportoinnista on myös hyötyä järjestelmän resurssien käytön seuraamisessa ja toiminnan optimoinnissa.

IPS:n toiminnan seuraaminen ja kokonaiskuvan muodostaminen sen toiminnasta ovat tärkeitä niin järjestelmän ylläpidon kuin asiakkaankin kannalta. IPS:n pitää tarjota ylläpidolle mahdollisuus toiminnan reaaliaikaiseen valvontaan. Vastaavanlainen toiminnallisuus on hyvä voida tarjota asiakkaalle.

## 5.2 Toteutus

Toteutusvaiheessa valitaan käytettävä IPS-teknologia, jolla luotava tuote toteutetaan ja käsitellään teknologian ominaisuuksia sekä miten sillä vastataan suunnitteluvaiheessa määritettyihin vaatimuksiin. Valitun IPS-teknologian ominaisuuksista käsitellään siihen kuuluvien tunnisteiden kattavuutta ja toimintaa ja riskien arvon määritystä. Erilaisia tunnistejoukkoja tarjoamalla voidaan vastata asiakkaiden erilaisiin liikenteen suodatustarpeisiin. Tunnistejoukkojen käyttöön liittyviä haasteita käsitellään luvussa 5.2.4. Kaikkiin tilanteisiin IPS-teknologian mukana tulevat tunnisteet eivät todennäköisesti tarjoa ratkaisua, joten on tärkeää, että teknologia tarjoaa mahdollisuuden luoda omia tunnisteita.

Tunnisteisiin liittyvien ominaisuuksien lisäksi toteutusvaiheessa selvitetään keinot seurata IPS-järjestelmän toimintaa ja tarjota raportteja sen toiminnasta. Toteutusvaiheessa suoritetaan myös järjestelmän varsinainen käyttöönotto. Tässä yhteydessä luvussa 5.2.1 valittu IPS-teknologia ja siihen kuuluva laitteisto konfiguroidaan ja sijoitetaan olemassa olevaan verkkoinfrastruktuuriin.

### 5.2.1 Valittu IPS-teknologia

Eri verkkolaitevalmistajilla on lukuisia eri IDS- ja IPS-toteutuksia. Tässä yhteydessä käyttöönotettavaksi valittiin kaksi Ciscon ASA 5525-X-palomuuria, jotka toimivat samalla reunapalomuureina suojaten kaikki konesalissa olevat palvelut. Näihin laitteisiin IPS-toiminnallisuuden saa sovellusmoduulina [35]. Ciscon tuotteiden puolesta puhui yrityksen aiempi kokemus saman valmistajan laitteista. Erilaisia avoimen lähdekoodin ratkaisuja harkittiin myös, mutta ne olisivat vaatineet enemmän päivittäistä ylläpitotyö-

tä. Tämä olisi IPS-tuotteen elinkaaren myötä tullut kalliimmaksi kuin Ciscon teknologiasta aiheutuvat kulut.

Laitteita ajetaan aktiivi-passiivi-parina, jossa aktiivisen laitteen vikaantuessa liikenne ohjataan automaattisesti passiiviselle laitteelle, josta tulee samalla aktiivinen. Yksittäinen ASA 5525-X pystyy prosessoimaan 1Gbps liikennettä palomuurin läpi [36]. Laitteessa toimiva IPS-moduuli taas pystyy prosessoimaan maksimissaan 400Mbps liikennettä [36]. Näin ollen kaikkea palomuurille tulevaa liikennettä ei voida ohjata IPS-moduulille. Tilanteen vaatiessa aktiivi-passiivi-pari voidaan muuntaa myös aktiivi-aktiivi-pariksi, mutta tätä ei vielä otettu lisenssien hintojen vuoksi käyttöön.

Koska IPS tuli sijoittumaan reunapalomuureille, kulkee kaikkiin sisäverkon kohteisiin tuleva liikenne sen kautta. Sisäverkon sisäinen liikenne kulkee ainoastaan sisäverkon kytkimien kautta ohittaen reunapalomuurin kokonaan. Sisäverkon kanssa olisi siis periaatteessa mahdollista käyttää erillistä IPS-sensoria, mutta toisaalta sisäverkon liikenteestä halutut osat voidaan tarvittaessa kierrättää myös reunapalomuurin kautta, jolloin erillisen sensorin tarve poistuu. Ciscon tarjoama IPS-ratkaisu mahdollistaa myös ulkoisten sensorien käytön, mikä tarvittaessa tarjoaa ratkaisun sisäverkon tunkeutumisen estoon ja havainnointiin. IPS-ratkaisua voi myös käyttää työasemien liikenteen suojaamiseen, mutta tämän työn puitteissa keskitytään ainoastaan verkkopalveluiden suojaamiseen.

### 5.2.2 Ciscon toimittamat tunnisteet

Ciscon IPS-teknologian mukana tulee automaattisesti päivittyvä joukko tunnisteita. Tällä hetkellä tunnisteita on tarjolla yli 9000 [37]. Tämä ei kuitenkaan tarkoita, että Ciscon IPS olisi suoraan paketista otettuna sopiva kaikkiin tilanteisiin. Tunnisteiden kattavuudesta ei myöskään ole tarkkaa tietoa.

Osa tunnisteista kohdistui järjestelmiin, joita ei sijainnut reunamuurien takana. Siten niiden käyttäminen oli turhaa ja aiheutti turhaa kuormaa IPS-moduuleilla. Koska käytännössä ainoastaan HTTP ja HTTPS liikenne on sallittua palomuurien läpi, kannatti tunnisteissa priorisoida portteihin 80 ja 443 kohdistuvia uhkia. Tässä yhteydessä havaittiin, että suojattavien kohteiden joukossa oli myös joitakin järjestelmiä, joihin kohdistuviin uhkiin Ciscon tunnisteet eivät tarjonneet suojaa. Havaitut uhat olivat varsin spesifejä ja niihin oli tarjolla muita korjauksia, mutta tämä osoitti, että myös omien tunnisteiden luominen on tietyissä tilanteissa tarpeen.

Myöskään tietoa järjestelmän oletusasetuksilla torjumista uhista ei ole saatavilla. Olemassa olevia tunnisteita voi kuitenkin selata ja hakea eri parametreilla[37]. Taulukossa kaksi on kuvattu eri hakusanoilla saatujen tunnisteiden lukumääriä ja julkaisuajankohtia. Taulukon haut on tehty marraskuussa 2015.

| Hakusana | Tulosten lukumäärä | Tuorein julkaisuajankohta |
|---|---|---|
| ssl | 47 | 28.5.2015 |
| httpd | 4 | 13.5.2015 |
| magento | 2 | 16.11.2015 |
| mysql | 25 | 26.3.2014 |
| dos | 337 | 4.11.2015 |
| atlassian | 5 | 7.10.2014 |
| liferay | 0 | - |
| java | 98 | 3.11.2015 |
| tcp | 603 | 3.11.2015 |
| icmp | 53 | 27.5.2014 |
| worm | 80 | 24.6.2015 |

***Taulukko 2.*** *Ciscon tunnisteiden lukumäärät hakusanoilla*

Saaduista luvuista voidaan havaita, että tiettyjen sovellusten, kuten Magenton ja Liferayn haavoittuvuuksia vastaan ei ole valmiita tunnisteita saatavissa. Alemman tason haavoittuvuudet, joita löytyy esimerkiksi SSL:n toteutuksista tai Javasta ovat paremmin Ciscon tunnisteilla havaittavissa. Näistä luvuista voidaan todeta, että sovelluskohtaiset haavoittuvuudet tulee edelleen pääsääntöisesti pyrkiä paikkaamaan, vaikka liikenne kulkisi Ciscon IPS:n läpi. Kun ollaan tilanteessa, jossa tiettyä haavoittuvuutta ei voida suoraan sovelluksessa korjata, IPS voi tarjota väliaikaisen ratkaisun sovelluksen suojaamiseksi.

Huomionarvoisa seikka on, että osa Ciscon tarjoamista tunnisteista on oletuksena poissa käytöstä. Nämä tunnisteet voivat vaikuttaa laitteiston toimintakykyyn negatiivisesti, ja niitä kannattaa ottaa käyttöön vain tarvittaessa [38].Oletusarvoisesti pois käytöstä olevat tunnisteet kannattaa käytännössä käydä läpi, koska joukossa todennäköisesti on tunnisteita, jotka kannattaa ottaa käyttöön. Oletuksena käytöstä on poissa esimerkiksi erilaisia palvelunestohyökkäyksiä koskevia tunnisteita ja esimerkiksi Slowloris-hyökkäykseen reagoiva tunniste. Jos kyseessä on kuitenkin tilanne, jossa IPS:llä ollaan suojaamassa lähinnä verkkoselaimella käytettäviä verkkopalveluita, voi Slowlorikselta suojautuminen olla täysin perusteltua.

### 5.2.3 Riskin arvon määritys ja käyttö

Luvussa 3.5 kuvattiin malli, jolla hyökkäysten, ja niiltä suojautumisen, kustannuksia voitiin arvioida. Ciscolla on tähän tarkoitukseen oma malli, jota IPS-järjestelmä käyttää [39].

Mallissa määritellään kuusi arvoa, joiden avulla saadaan laskettua riskin arvo (Risk Rating, RR). Tunnisteen tarkkuusarvo (Signature Fidelity Rating, SFR) kertoo, kuinka todennäköisesti tunnisteeseen liittyvä tapahtuma on uhka. Mitä suurempi arvo, sitä todennäköisempi uhka on. Hälytyksen vakavuusarvo (Alert Severity Rating, ASR) kuvaa hyökkäyksestä aiheutuvan vahingon määrää. Cisco on etukäteen määritellyt jokaiselle tunnisteelle tällaisen arvon neljästä mahdollisesta, mutta loppukäyttäjä voi myös muuttaa arvoa. Kohteen arvo (Target Value Rating, TVR) taas antaa käyttäjän määrittää suojattaville kohteille erilaisia arvoja, jolloin niitä painotetaan IPS:n toimesta eri tavalla. Neljäntenä arvona on hälytyksen merkityksellisyysarvo (Alert Relevancy Rating, ARR), joka on IPS:n muodostama käsitys kohteen haavoittuvuudesta havaitulle uhalle.Tämä perustuu IPS:n tietoihin kohteen käyttöjärjestelmästä ja siitä onko IPS suoraan liikennevirrassa vai ei [40]. Liikennevirran ulkopuolelle sijoitettu IPS ei ole Ciscon mukaan aivan yhtä tarkka kuin suoraan liikennevirtaan sijoitettu [39]. Tämä epätarkkuus huomioidaan kopioinnin muutosarvolla (Promiscuous Delta, PD), joka vähennetään riskin arvosta, mikäli IPS ei ole suoraan liikennevirrassa. Viimeisenä vaikuttavana arvona on tarkkailulistan arvo (Watch List Rating, WLR). Tämä arvo muodostuu erillisten Ciscon tietoturva-agenttien toimittaman datan perusteella. Käytännössä tarkkailulista koostuu IP-osoitteista, joiden tietoturva-agentti on havainnut olleen osallisina palvelimeen kohdistuneisiin hyökkäyksiin tai tiedusteluun. Mikäli havaitun hyökkäyksen lähdeosoite on tällä listalla, lisätään WLR:n arvo riskin arvoon. Näiden arvojen avulla saadaan Ciscon mukaan laskettua riskin arvo seuraavalla kaavalla [39]:

$$RR = \frac{SFR \times ASR \times TVR}{10000} + ARR - PD + WLR$$

SFR:n ja ASR:n vaihteluvälit ovat 0-100, mutta kohteen arvo voi vaihdella välillä 0-200. Tällä tavoin voidaan arvostaa kriittisimpiä järjestelmiä koskevia uhkia yli vähemmän kriittisten [39]. PD taas vaihtelee välillä 0-30 ja WLR välillä 0-35.ARR saa joko arvon -10, 0 tai 10 [40]. Ciscon mukaan Riskin arvo vaihtelee välillä 0-100, mutta yllä oleva kaava mahdollistaa kuitenkin vaihtelun välillä -45–245. Toisesta lähteestä tarkastettuna riskin arvon laskentaa tarjotaan myös hieman erilainen kaava [40]:

$$RR = \frac{SFR \times ASR \times TVR}{100 \times 100 \times 100} + ARR - PD + WLR$$

Tämän kaavan myötä riskin arvon vaihteluväli on -45–47. Ristiriitaisista tiedoista päätellen kaavoja ei ole tarkoitus ottaa täysin matemaattisesti, vaan ne ovat enemmänkin suuntaa antavia.

Riskin arvon suuruuteen voi vaikuttaa myös Ciscon Global Correlation. Tämä on Ciscon keräämään telemetriadataan perustuva tietokanta, jossa IP-osoitteille muodostuu maine niistä tehtyjen havaintojen perusteella. Ciscon laitteet lähettävät dataa havaituista hyökkäyksistä takaisin Ciscolle, jossa Cisco prosessoi tiedon, ja muodostaa sen perusteella arvon jolla riskin arvoa voidaan muokata liikenteen lähdeosoitteen perusteella. Global Correlationin voi halutessa ottaa pois päältä.Myös telemetriadatan lähettämisen voi estää, ja silti käyttää Ciscon muita Global Correlationin ominaisuuksia. [41]

RR on Ciscon IPS:n sisäisesti käyttämä arvo. Järjestelmä laskee sen itse edellä mainittujen parametrien perusteella. IPS:lle voidaan luoda erilaisia suotimia ja sääntöjä, jotka toteuttavat määriteltyjä asioita, jos uhan riskin arvo ylittää tietyn rajan. Esimerkiksi riittävän korkea RR voi yksistään riittää liikenteen estämiseen, vaikka hälytyksen vakavuus tai mikään muu yksittäinen arvo ei sitä edellyttäisikään. Cisco määrittelee oletuksena kolme luokkaa, johon uhat jaetaan RR:n perusteella. Nämä on esitetty taulukossa kolme.

| **Luokka** | **RR** |
|---|---|
| HIGHRISK | 90-100 |
| MEDRISK | 60-90 |
| LOWRISK | 0-60 |

***Taulukko 3.*** *Ciscon uhkien oletusluokat*

Järjestelmää käyttöönotettaessa luotiin vielä yksi luokka nimeltä MINRISK, jolle määriteltiin RR-rajoiksi 1-30. Tämän myötä LOWRISK:n arvoväliksi tuli 30-60 ja MEDRISK:lle 60-90. Samalla määriteltiin myös sääntö, joka estää lokituksen LOWRISK-luokkaan osuvilta hälytyksiltä.

### 5.2.4 Muokatut tunnisteet ja tunnistejoukot

Ciscon IPS:n sisäinen arkkitehtuuri mahdollistaa teoriassa vain yhden sääntöjoukon sitomisen yhteen virtuaaliseen tai fyysiseen sensoriin. Ciscon ASA:n IPS-moduulin tapauksessa käytössä on yhdestä neljään virtuaalista sensoria. Näistä jokaiseen voidaan määritellä tietynlainen sääntöjoukko. Palomuurilta liikenne ohjataan IPS-sensorille pääsynhallintalistalla (access control list). Tässä yhteydessä voidaan myös valita tarkemmin, mitä virtuaalisensoria käytetään. Näin ollen valitulla IPS-toteutuksella voidaan tarjota neljä erilaista sääntöjoukkoa. Koska määrä on näin rajallinen, niin asiakkaille ei

voi tarjota mahdollisuutta määritellä täysin omaa, vain heitä koskevaa sääntöjoukkoa. Sen sijaan on mahdollista luoda Ciscon tarjoaman sääntöjoukon lisäksi muita sääntöjoukkoja, joilla voi tarjota erilaista palvelua asiakkaille. On siis mahdollista tarjota sääntöjoukko, jolla suodatetaan esimerkiksi ainoastaan haitallisten bottien liikennettä.

Aina haavoittuvuuden korjaaminen ei ole mahdollista. Silloin on perusteltua paikata tilannetta laatimalla haavoittuvuuden tunnistava tunniste. Luotu tunniste pitää testata hyvin ennen käyttöönottoa tuotantoympäristössä. Yhden virtuaalisensorin varaaminen pysyvästi testikäyttöön voi jossain tilanteissa olla perusteltua. Tällöin uudet tunnisteet testattaisiin ensin tällä virtuaalisensorilla, jolle on ohjattu ainoastaan kulloinkin kohteena olevan palvelun liikenne. Kun tunniste on testattu toimivaksi, se voidaan ottaa käyttöön muidenkin sensorien kanssa ja siirtää siten tuotantokäyttöön.

### 5.2.5 Omien tunnisteiden luominen

Kuten luvussa 5.2.2. todettiin, Ciscon tarjoamat tunnisteet eivät automaattisesti tarjoa suojaa kaikkiin tilanteisiin. Alemman tason haavoittuvuudet ovat paremmin mukana tulleiden tunnisteiden kattamia kuin ainoastaan tiettyä sovellusta koskevat spesifimmät haavoittuvuudet. Sovelluskohtaiset haavoittuvuudet tulisi pyrkiä korjaamaan aina sovelluksessa, mutta liikenteen suodatus ennen sen pääsyä sovellukseen voi toimia väliaikaisena suojautumiskeinona Tällaisiin tilanteisiin omien, juuri tilanteeseen sopivien tunnisteiden luominen on yksi ratkaisu.

Tämän työn puitteissa luotiin tunniste yrityksen vanhasta tuotteesta löydettyyn haavoittuvuuteen. Koska kyseessä on itse kehitetty sovellus, siihen ei ole saatavissa valmista tunnistetta. Kyseinen sovellus on myös niin vanha, että sitä ei enää aktiivisesti kehitetä, joten haavoittuvuutta ei myöskään pystytä korjaamaan nopeasti. Haavoittuvuus mahdollistaa HTTP-injektion sovellukseen, jolloin hyökkääjä voi esimerkiksi sopivan linkin avulla tarjota aidonnäköisen kirjautumissivun, joka huijaa käyttäjän luovuttamaan käyttäjätunnuksensa hyökkääjälle. Haavoittuvuutta varten luotu tunniste on esitelty liitteessä A.

Tunnisteen luomiseksi täytyi haavoittuvuuden toiminta ensin ymmärtää. Tämä oli tehty jo etukäteen, kun haavoittuvuus oli havaittu. Haavoittuvuus mahdollistaa kommentin sulkemisensekä ajettavan koodin injektoinnin ja suorituksen sivulatauksen yhteydessä. Tämä onnisuu ainoastaan yhden parametrin kanssa, joten mikäli kommentin sulkeminen parametrin arvossa estetään, niin haavoittuvuutta ei voi hyödyntää. Tämän estäminen onnistuu IPS:llä, sopivalla tunnisteella. Tunnisteet muodostetaan määrittelemällä mahdollisimman paljon haavoittuvuutta käyttävän hyökkäyksen tunnusmerkkejä. Tällaisia tässä tapauksessa olivat liikenteen portti, käytetty protokolla, haavoittuvan parametrin tarkka polku ja sen arvoksi annettu html-kommentin päättävä merkkijono, joka viimeistään on merkki yrityksestä käyttää haavoittuvuutta. Näistä tunnusmerkeistä helppoja määriteltäviä ovat käytetty portti ja protokolla, mutta parametrin polun ja parametrille

annetun arvon tarkastelu vaativat säännöllisten lausekkeiden (regular expression) käyttöä. Näiden laatiminen ja testaaminen ovat tunnisteen laatimisessa työläin vaihe. Huonosti laadittu ja testattu tunniste tuottaa vääriä positiivisia, ei välttämättä suojaa kaikilta tavoilta hyödyntää haavoittuvuutta tai pahimmassa tapauksessa haitata suojattavan kohteen luvallista käyttöä.

Omien tunnisteiden luominen on siis mahdollista ja niillä voidaan parhaimmillaan suojata nopeasti kaikki tietystä haavoittuvuudesta kärsivät sovellukset, joiden liikenne kulkee IPS:n läpi. Toisaalta tunnisteen luominen joitakin haavoittuvuuksia varten voi olla todella aikaa vievää, jos käsiteltävänä on useita eri parametreja, tai haavoittuvuuden hyödyntämiseen liittyvää liikennettä on vaikea erottaa luvallisesta liikenteestä.

### 5.2.6 Toiminnan seuranta ja raportointi

IPS-moduuli ei yksistään tarjoa mitään raporttia toiminnastaan, mutta se pystyy kuitenkin tarjoamaan dataa havaitsemistaan hyökkäyksistä SDEE-standardin mukaisesti. SDEE on ICSA:n (International Computer Security Association) omistama standardi, joka määrittelee XML:ään (Extensible Markup Language) perustuvan formaatin IDPS-laitteiden hälytyksille [42]. SDEE:llä on siis mahdollista hakea havaittuja hyökkäyksiä koskevaa dataa IPS:ltä, ja parsia sitten saadusta XML-muotoisesta datasta halutunkaltainen raportti. Tätä ei tämän työn puitteissa selvitetty tarkemmin, mutta tiedostimme mahdollisuuden tällaiseen.

IPS-moduulin toimintaa on mahdollista seurata sen hallintatyökalulla Cisco Intrusion Prevention System Device Managerilla. Pelkkään toiminnan seurantaan hallintatyökalu ei kuitenkaan ole paras ratkaisu sen kankeudesta vuoksi.Se kuitenkin riittää ylläpidon tarpeisiin, kunhan SNMP-pohjainen automaattinen valvonta on myös olemassa.

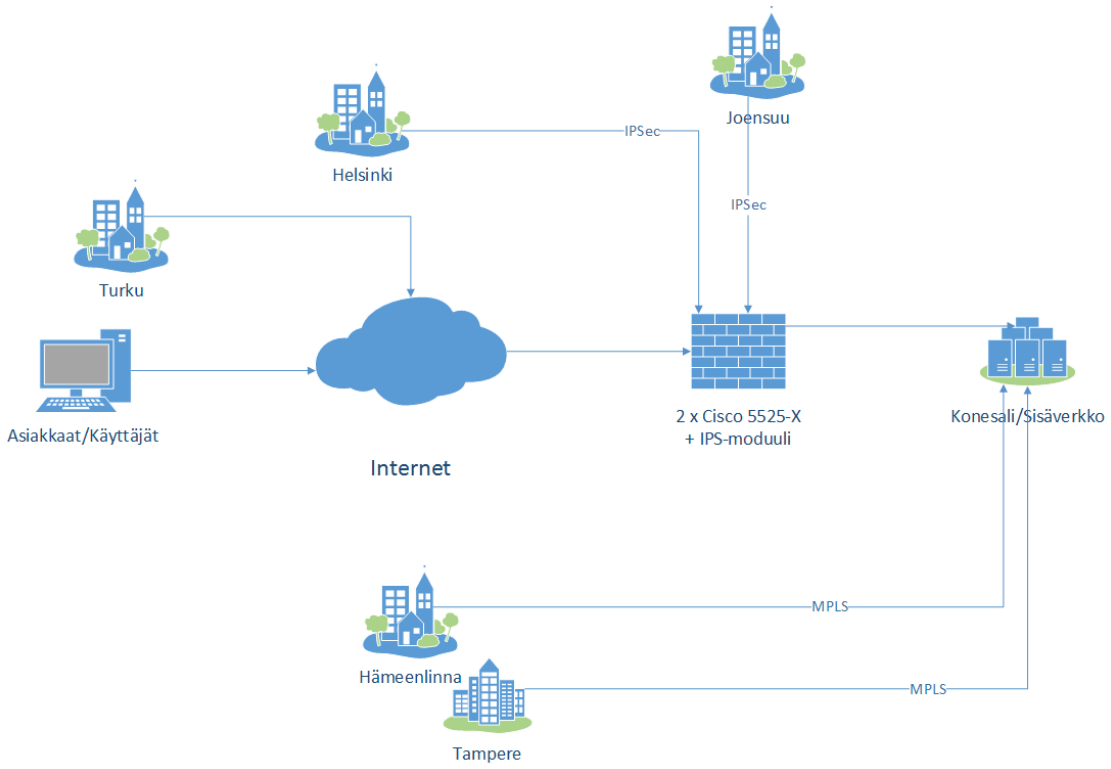
Asiakkaille IPS:n toiminnan seuraaminen on ongelmallisempaa. Asiakkaan tulisi nähdä ainoastaan omia palveluitaan koskevat tapahtumat, mutta hallintatyökalu ei mahdollista näin hienovaraista oikeuksien jakamista. Paras vaihtoehto tämän toteutukseen onkin käyttää jotain ulkopuolista järjestelmää joka hakee IPS:n toimintadataa SDEE:llä, ja parsii sitten siitä ainoastaan asiakkaan järjestelmiä koskevan datan sopivaan esitysmuotoon.

Tällaiseen käyttöön sopivaa sovellusta ei markkinoilta suoraan löydy, ja tämän työnpuitteissa asiaa ei selvitetty pidemmälle.

### 5.2.7 IPS-laitteiden käyttöönotto

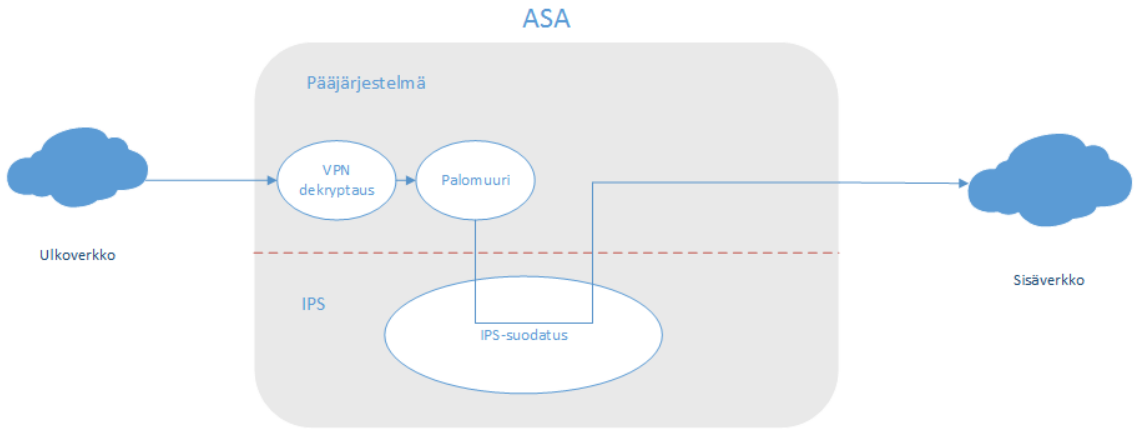
Kuten luvussa 5.2.1. mainitaan, IPS-toiminnallisuutta toteutetaan reunapalomuureilla olevilla IPS-moduuleilla. Verkkotopologiaa on kuvattu kuvassa seitsemän. Järjestelmän käyttöönoton kannalta tämä osoittautui hidasteeksi. Koska IPS-moduulit toimivat tuo-

tantopalomuurien yhteydessä, vaadittiin niiden konfigurointiin huolellisuutta, jotta palomuurien normaali toiminta ei häiriydy. Erillisen testiympäristön perustaminen ei ollut järkevää ajankäyttöön ja lisensointiin liittyvien syiden vuoksi. Tuotantopalomuurit toimivat aktiivi-passiivi-parina, joten IPS-moduulin käyttöönottoa oli turvallisempaa suorittaa aluksi passiivisella palomuurilla. Tällöin mahdolliset ongelmat eivät olisi päässeet vaikuttamaan tuotantodatan liikenteeseen.




***Kuva 7:*** *Yrityksen verkkotopologia*

Palomuurin yhteydessä toimiva IPS jakaa samat fyysiset verkkoliitännät isäntälaitteen kanssa. Laitteelle tuleva liikenne tulee ensin palomuuriohjelmiston käsiteltäväksi, jonka jälkeen haluttu liikenne ohjataan IPS-moduulin käsiteltäväksi [35]. Tätä toimintaa on havainnollistettu kuvassa kahdeksan. Tässä kohtaa voidaan määrittää, mitä IPS:n neljästä virtuaalisesta sensorista käytetään, ja sijoitetaanko IPS suoraan liikennevirtaan, vai lähetetäänkö sille ainoastaan kopio liikenteestä




***Kuva 8:*** *IPS-moduulin käyttö palomuurissa, mukailtu [35]:stä*

Käyttöönotto suoritettiin vaiheittain.Aluksi pyrittiin saamaan IPS-moduulit toimimaan oletusasetuksilla häiritsemättä muuta liikennettä. Tämän jälkeen moduuleille ohjattiin valituille demopalveluille kulkevaa liikennettä, jotta saadaan näyttöä IPS:n toiminnasta ja voidaan varmistaa oletussääntöjen toiminta. Kun oletussäännöt oli todettu toimiviksi, aloitettiin laitteen konfiguraation perusteellisempi täydennys. Tässä kohtaa laitettiin kuntoon muun muassa automaattiset tunnistepäivitykset, moduulin generoimat hälytykset ja toiminnan valvonta. Samalla moduuleille ohjattiin myös joidenkin sisäisten palveluiden liikennettä, jotta moduulien suorituskyvystä ja toiminnasta saadaan enemmän dataa. IPS:n toimintaa päätettiin seurata joidenkin viikkojen ajan, ja muokata asetuksia tarpeen mukaan. Tälle vaiheelle ei asetettu mitään absoluuttista takarajaa, koska IPS:n varsinaisen tuotantokäytön aloitukselle ei myöskään ollut sellaista. Lopulta, kun moduulien oikeanlainen toiminta oli varmistettu, oli järjestelmä valmis käyttöön myös asiakkaiden järjestelmien kanssa. Käyttöönoton vaiheita on havainnollistettu taulukossa neljä.

| |
|---|
| 1. IPS-moduulien käyttöönotto ilman haittaa muulle liikenteelle |
| 2. Testidatan ohjaaminen IPS-moduulille |
| 3. Konfiguraatioiden täydennys |
| 4. Toiminnan tarkkailu ja konfiguraation optimointi |
| 5. Käyttöönotto tuotantodatan kanssa |

***Taulukko 4.*** *IPS:n käyttöönoton vaiheet*

Käyttöönotto ei merkinnyt tuotteen kehityksen loppua, vaan erilaista optimointia oli edelleen mahdollista tehdä. Tavoitteena oli muovata IPS:n toimintaa vielä enemmän

halutun mallin mukaiseksi ja kartoittaa mahdollisuuksia tarjota asiakkaille erilaisia enemmän räätälöityjä IPS-tuotteita.

## 5.3 Ylläpito

Ylläpitovaihe on pisimpään kestävä vaihe tuotteistuksessa. Sen voidaan katsoa alkavan, kun toteutusvaihe on saatu päätökseen ja IPS on otettu käyttöön tuotannossa olevien palveluiden kanssa.

Tässä luvussa käsitellään sitä, millä tavoin ylläpitovaiheeseen varaudutaan, ja millaisiin asioihin sen jokapäiväisessä käytössä tarvitsee varautua, vaikka järjestelmä olisikin konfiguroitu tilanteeseen sopivasti ja toiminta olisi pääosin automaattista. Aluksi käsitellään henkilöstöön ja sen osaamiseen liittyviä seikkoja luvussa 5.3.1. Tämän jälkeen, luvussa 5.3.2 käsitellään IPS:n toiminnan valvontaa ja siihen liittyviä jokapäiväisiä prosesseja. Lopuksi käsitellään vielä IPS-toteutuksen päivittämiseen liittyviä toimia ja riskejä.

### 5.3.1 Henkilöstö

Käyttöönotetun IPS-teknologian kanssa päivittäin toimivan henkilöstön täytyy hallita sen käyttöä riittävästi. Luvussa 2.9.3 esiteltiin keinoja, joista tarvittavaa tietämystä voidaan hankkia. Näistä tärkeimmät ovat valmistajan tai yhteistyökumppanin järjestämät koulutukset ja valmistajan tarjoama dokumentaatio. Näillä kahdella saavuttaa todennäköisesti riittävän kattavan tietämyksen, joka riittää IPS:n päivittäiseen operointiin.

Tämän työn puitteissa IPS-järjestelmän konfigurointiin ja käyttöönottoon tutustuttiin aluksi Ciscon oman ja kolmansien osapuolien laatiman dokumentaation avulla. Varsinainen dokumentaatio laitteen eri ominaisuuksien konfigurointiin oli kattavaa, mutta dokumentoituja esimerkkitoteutuksia ja parhaita toimintatapoja ei ollut kuvattu riittävästi. Näin ollen ennen käyttöönottoa päätettiinkin hankkia Ciscon virallisen partnerin tarjoama koulutus IPS:n käyttöön. Koulutukseksi valikoitui viisi päivää kestävä Implementing Cisco Threat Control Solutions -koulutus muokattuna ja tiivistettynä yrityksen tarpeisiin. Koulutuksen yhteydessä konfiguraatiota testattiin erillisessä koulutusympäristössä. Saadut materiaalit tarjosivat esimerkkejä ja malleja IPS-järjestelmän oikeaan käyttöönottoon.

### 5.3.2 Toiminnan valvonta

IPS:n toiminnan valvonnan tulee olla mahdollisimman automaattista, ja hälytystasojen säädetty siten, että ainoastaan oikeasti henkilöstön reagointia vaativista asioista tulee ilmoitus. Jokaisesta estetystä tapahtumasta ei ole tarpeen saada ilmoitusta.

Koska IPS-toiminnallisuus tapahtuu palomuurien yhteydessä olevalla erillisellä sovellusmoduulilla, toteutuu osa sen valvonnoista suoraan palomuurien kautta. Esimerkiksi

palomuurit havaitsevat moduulien uudelleenkäynnistykset ja ilmoittavat niistä SNMP:llä. Moduulin sisäisen toiminnan ja raja-arvojen valvonta vaatii kuitenkin myös IPS-moduulin valvontaa. Tämä oli mahdollista toteuttaa myös SNMP:llä [43]. Kun SNMP saatiin konfiguroitua IPS-moduuleille, koordinoitiin valvontojen luominen valvontapalveluiden tarjoajan kanssa, jotta valvonta saatiin hälyttämään oikeanlaisista asioista.

IPS-moduulin toiminnan valvonnan lisäksi haluttiin hälytykset käynnissä olevista hyökkäyksistä, jotka vaativat muuta reagointia ylläpidolta. Kaikista IPS:n havaitsemista ja estämistä hyökkäyksistä ei ole mielekästä saada ilmoitusta, joten hälytysrajat piti konfiguroida tunnistekohtaisesti. IPS-moduuli mahdollisti hälytykset käyttämällä SNMP:n TRAP-viestejä. Aktiivisten tunnisteiden joukosta valittiin kriittisimmiksi katsotut tunnisteet, ja konfiguroitiin ne lähettämään TRAP-viestit valvonta-agentille, joka luo niiden perusteella hälytyksen valvontaportaaliin.

### 5.3.3 Järjestelmän päivitykset

IPS:n valvonnan lisäksi oli suunniteltava prosessi IPS:n järjestelmäpäivityksien asentamiseen. Ciscon IPS-moduulin tapauksessa päivityksiä on kahdenlaisia. Kohdassa 5.2.2. mainittujen tunnistepäivitysten lisäksi koko IPS-moduulin sovellusversioon ilmestyy ajoittain päivityksiä. Näiden päivitysten asennus oli syytä suunnitella ja testata ennen tuotantokäyttöä, koska päivityksen asennus aiheuttaa katkon moduulin toimintaan.

Cisco ei tarjonnut varsinaista ohjetta päivityksien tekoon aktiivi-passiivi-laiteparilla, joten päivityssuunnitelma laadittiin testauksen pohjalta. Testauksen tuloksena havaittiin, että järjestelmäpäivitykseen liittyvä IPS-moduulin uudelleenkäynnistys näkyy palomuurille vastaavasti kuin IPS-moduulin vikaantuminen. Mikäli IPS-moduuli päivitetään aktiivi-passiivi-parin aktiivisella laitteella, aktiivinen laite havaitsee itsessään laitevian ja käynnistää korjausmekanismin, jonka avulla se siirtyy passiiviseksi laitteeksi, kun taas passiivinen laite ottaa aktiivisen roolin. Tämä on normaali tapa, jolla aktiivi-passiivi-pari toimii, mutta korjausmekanismin käyttöön liittyy aina pieniä riskejä aukinaisten yhteyksien ja istuntojen virheettömän siirtämisen suhteen. Tästä syystä päätettiinkin, että IPS-moduulin päivitykset pyritään tekemään aina palomuurin järjestelmäpäivitysten yhteydessä, jolloin aktiivinen laite vaihtuu joka tapauksessa. Tällöin IPS:n järjestelmäpäivitys asennetaan ensin passiiviselle laitteelle, jonka jälkeen päivitetään palomuurien järjestelmät, ja aktiivinen laite vaihtuu, minkä jälkeen päivitetään IPS myös toiselle laitteelle.

## 5.4 Elinkaaren hallinta ja kehitys

Tässä luvussa käsitellään luotavan IPS-tuotteen elinkaaren hallintaa ja kehitystä. Tuotteeseen on toteutusvaiheessa valittu käyttöön IPS-teknologia, jolla tuote on toteutettu,

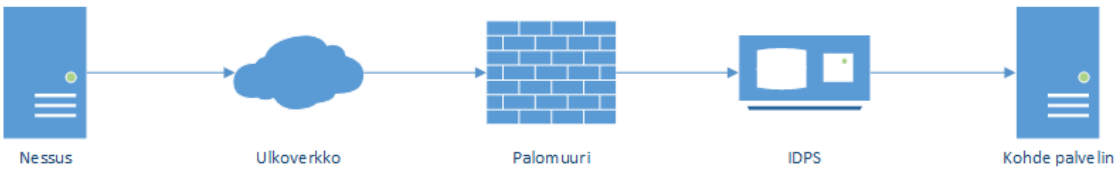
mutta tämän teknologiavalinnan ei tarvitse olla pysyvä.Se voidaan, ja mahdollisesti myös täytyy, korvata jossain vaiheessa toisella teknologialla. Varsinaisen asiakkaalle tarjottavan tuotteen ei tarvitse muuttua, mutta teknologian vaihdolla voidaan myös pyrkiä vastaamaan asiakkailta tulleisiin toiveisiin tuotteen kehityksen suhteen. Tällaisia teknologia valintoja varten on hyvä selvittää, miten hyvin nykyinen teknologia toimii ja mitä ongelmia siinä on. Näitä asioita on käsitelty luvuissa 5.4.1 ja 5.4.2.Luvussa 5.4.3 käsitellään tämän hetkisen tuotteen tilannetta, ja arvioidaan, mitä muutoksia ja minkälaisella aikataululla sen suhteen täytyy tehdä.

### 5.4.1 Tuotteen suorituskyvyn mittaus

IDS-tuotteiden ja järjestelmien toiminnan ja suorituskyvyn arviointiin ei ole olemassa standardoitua menetelmää. Zuech ym. mukaan suurin ongelma IPS-järjestelmien suorituskykyjen vertailussa, on yhteisen mitta-asteikon ja sopivan reaalidataan perustuvan testidatan puute [44]. Tällaisen datan puuttuessa testattiin järjestelmän tarkkuutta tietoturvaskannerilla.

Testaus tehtiin Tenable Network Securityn Nessus Professional-tietoturvaskannerilla. Tenable ei tarjoa tarkkoja lukuja siitä, kuinka monta erilaista uhkaa ja haavoittuvuutta skannerilla voi testata. Markkinointimateriaalit lupaavat kuitenkin hyvin kattavaa skannausta, jossa käsitellään muun muassa palvelinalustat, verkkosovellukset ja tietokannat [45]. Skanneria voidaan tämän perusteella pitää riittävän kattavan, IPS:n testauksen tarpeisiin.

Nessus sijaitsee yrityksen verkon näkökulmasta ulkoverkossa, joten sieltä tulevat yhteydet ovat palomuurin ja IPS:n näkökulmasta kuten mitä tahansa ulkoverkosta tulevaa liikennettä. Näin ollen liikenne kulkee ensin palomuurin ja sitten IPS:n läpi, kuten kuvassa kahdeksan on esitetty.




***Kuva 8.*** *Nessuksen käyttö tietoturvaskannaukseen*

Testiä varten asennettiin palvelin, jonne asennettiin Wordpress 3.0 ja sen vaatima sovelluspino, johon kuului MySQL 5.1, Apache Httpd ja PHP 5.1. Palvelinalustana toimi Red hat Enterprise Linux 6.7. Palvelin ja palvelu skannattiin tietoturvaskannerilla kahdesti, aluksi ilman minkäänlaista suojausta, eli ilman palomuuria tai IPS:ää. Tämän jälkeen skannaus ajettiin uudelleen, kun pelkkä IPS oli käytössä. Tulokset on nähtävissä taulukossa kuusi.

Jotta IPS:n suorituskykyä ja tarkkuutta saatiin testattua, ajettiin Nessuksen skannaus tiettyä kohdetta kohti ensin ilman palomuuria ja IPS:ää, jotta saatiin Nessuksen raportti täysin suojaamattomasta palvelimesta. Tämän jälkeen sama testi toistettiin ensin pelkän palomuurin kanssa ilman IPS:ää, sitten pelkän IPS:n kanssa ilman palomuuria ja lopuksi sekä palomuurin että IPS:n kanssa. Näiden perusteella saatiin taulukossa viisi olevat tulokset.

| | Vakavat haavoittuvuudet | Keskitason haavoittuvuudet | Lievät haavoittuvuudet | Tietoturvailmoitukset |
|---|---|---|---|---|
| IPS | 0 | 1 | 0 | 14 |
| Ei IPS:ää | 0 | 1 | 2 | 22 |

***Taulukko 5.*** *Nessuksen löytämät haavoittuvuudet*

Taulukon tuloksista voidaan havaita, että palvelinalusta itsessään on jo varsin turvallinen täysin ilman palomuuriakin. Vakavia haavoittuvuuksia ei löytynyt, ja keskitasoisiakin vain yksi. IPS:n toiminta voidaan kuitenkin havaita, sillä skanneri ei pystynyt havaitsemaan kumpaakaan lievää haavoittuvuutta IPS:n ollessa toiminnassa, ja tietoturvailmoitustenkin määrä laski yli kolmanneksella. Huomionarvoista on myös, että skannaukseen kulunut aika moninkertaistui, kun IPS oli suojaamassa palvelua.

Tämän lisäksi vastaavanlainen testi toteutettiin myös Acunetix-tietoturvaskannerilla. Acunetix on verkkosovellusten haavoittuvuuksiin keskittynyt tietoturvaskanneri, joten se tarjoaa paremman kuvan sovellustasolla torjutuista uhista, kuin Nessus, joka tarkastelee skannattavaa palvelinta kokonaisvaltaisemmin[46].

Acunetixillä skannattiin samaa palvelua kuin Nessuksella. Skannausta varten laadittiin profiili, joka tarkasteli erityisesti Wordpress-sovellukseen kohdistuvia haavoittuvuuksia. On huomionarvoista, että asennettu Wordpressin versio on tarkoituksella vuodelta 2010 [47]. Tämän vuoksi siinä voidaan olettaa olevan paljon haavoittuvuuksia. Suoritettujen skannausten tulokset ovat nähtävissä taulukossa kuusi. Skannausraportit löytyvät liitteinä B ja C.

| | Vakavat haavoittuvuudet | Keskitason haavoittuvuudet | Lievät haavoittuvuudet | Tietoturvailmoitukset |
|---|---|---|---|---|
| IPS | 19 | 3 | 1 | 1 |
| Ei IPS:ää | 20 | 3 | 6 | 1 |

***Taulukko 6.*** *Acunetixin löytämät haavoittuvuudet*

Acunetixin skannaus osoittaa, että oletuksena päällä olevat tunnisteet eivät pääsääntöisesti tarjoa turvaa riittävän vanhoihin haavoittuvuuksiin. On myös mahdollista, että tapa, jolla Acunetix suorittaa skannauksen, perustuu täysin tai osittain jonkin metatiedon käyttöön, eikä se suoranaisesti yritä toteuttaa haavoittuvuutta käyttävää hyökkäystä. Eli

Acunetix voi siis esimerkiksi pyrkiä selvittämään kohteena olevan sovelluksen version ja päätellä sen perusteella sovelluksen olevan tietyllä tavalla haavoittuva. Skannauksen aikana IPS:n lokista oli kuitenkin nähtävissä joihinkin tunnisteisiin osuvia hyökkäyksiä. Näistä kaikki eivät tosin laukaisseet liikenteen estoja, joten ne näkyvät skannaustuloksissa edelleen havaittuina haavoittuvuuksina.

Yhteenvetona tietoturvaskannausten tuloksista voidaan sanoa, että IPS:n käyttäminen parantaa suojattavien palveluiden tietoturvaa ja sillä on mahdollisuus puuttua suojattavissa palveluissa oleviin tietoturvapuutteisiin. Järjestelmän lokeista oli skannauksien jälkeen nähtävissä, mitä kaikkea skannauksen yhteydessä järjestelmän näkökulmasta oli tapahtunut ja miten siihen oli reagoitu. Esimerkiksi erilaiset porttiskannaukset saatiin järjestelmällä kiinni. Pelkästään tieto tällaisista ja niiden toistuvuudesta voi olla asiakkaalle arvokas.

Tietoturvaskannerilla tehty testaus ei anna parasta mahdollista kuvaa IPS-järjestelmän toiminnasta, sillä se ei testaa oikeita asioita Skanneri ei pyri jäljittelemään oikeaa palveluun kohdistuvaa liikennettä, joten sillä suoritettua testausta ei voi käyttää väärien positiivisten tunnistamiseen. Pelkällä tietoturvaskannerilla tehdyn testauksen yhteydessä onkin suuri kiusaus säätää IPS:n asetuksia tiukemmalle, jotta saadaan suurempi määrä skannerista aiheuttavaa haittaliikennettä estettyä. Samalla kuitenkin todennäköisyys vääriin positiivisiin kasvaa, ja hyöty palvelun turvallisuuden kannalta jää kyseenalaiseksi.

Skannauksella ei saatu aikaan näkyvää kuormaa IPS:n suorituskykymittauksessa. Käytännössä mittauksissa näkyvän kuorman luominen vaatisi merkittävästi enemmän liikennettä, kuin yksittäinen tietoturvaskannaus pystyy tuottamaan. Kuormitustestausta ei lähdetty tämän työn puitteissa suorittamaan, sillä siitä ei saada IPS-tuotteen kannalta oleellista tietoa. Laitteen kuormaa pitää kuitenkin valvoa aktiivisesti ja sen muutoksiin tulee reagoida..

### 5.4.2 Valitun ratkaisun ongelmat

Erilaisten IPS-ratkaisuiden suurimpia rajoitteita on salatun liikenteen käsittely. Esimerkiksi tavalliseen HTTPS:ää käyttävän verkkopalvelun suojaaminen IPS:llä on ongelmallista, koska niin laillinen liikenne kuin laitonkin on salattua. Tällöin IPS ei pääse näkemään ja prosessoimaan liikennettä. Ratkaisuna tällaiseen on purkaa yhteyden salaus jo ennen IPS:ää. Tällöin voidaan esimerkiksi rakentaa palomuurin jälkeen kuormantasauskerros, joka purkaa SSL-suojauksen, ja sen jälkeen ohjata liikenne IPS:lle. Tällainen ratkaisu on kuitenkin hankalampi, kun käytössä on palomuurin yhteydessä toimiva IPS-moduuli. Tämän työn puitteissa salatun liikenteen käsittelyyn liittyvää ongelmaa ei ratkaistu, mutta ratkaisuvaihtoehtoja kartoitettiin.

IPS-järjestelmät pystyvät torjumaan tietynlaisia palvelunestohyökkäyksiä. Kuten luvussa 5.2.2 todetaan, Ciscolta löytyy tunnisteet satoihin erilaisiin palvelunestohyökkäyksiin. Kuitenkin liikenteen määrän kasvaessa riittävän suureksi, järjestelmän prosessointikapasiteetti tulee vastaan. Tämän vuoksi IPS ei yksistään ole täydellinen ratkaisu palvelunestohyökkäyksiä vastaan, eikä se sillä tavoin korvaa Elisan Kilpi-palvelun kaltaisia palveluita.

Valitussa Ciscon IPS-toteutuksessa oli puutteita toiminnan seuraamisen suhteen. Hyödyllinen, mutta puuttuva ominaisuus olisi ollut lokitietojen kerääminen keskitetysti johonkin ulkoiseen järjestelmään Syslog-standardin mukaisesti. Sen sijaan tämä data saadaan laitteesta ulos SDEE-protokollaa käyttäen, kuten luvussa 5.2.6 esiteltiin.

Toisena ongelmana Ciscon toteutuksessa oli raportointiominaisuuksien puute. IPS:n havaitsemista tapahtumista ja suorittamista toimenpiteistä olisi hyvä saada koostettua raportteja. Tällaisten avulla voisi helposti seurata, millaista tiedustelua suojattavia palveluita kohtaa tehdään, ja muokata IPS:n konfiguraatiota tarpeen mukaan. Raporteilla olisi myös helppo osoittaa asiakkaille, millaista haittaliikennettä heidän palveluaan kohti on havaittu.

### 5.4.3 Tuotteen jatkuvuuden hallinta

IPS-tuotteen jatkuvuuteen suurin vaikuttava ulkoinen tekijä on nykyisen teknologian elinkaari. IPS-teknologioita tarjoavat tahot kehittävät omia tuotteitaan ja palveluitaan jatkuvasti, joten mikään käyttöön valittu teknologia ei ole ikuinen, ja uusia vaihtoehtoja tulee säännöllisesti markkinoille. Muiden teknologioiden kehitystä kannattaa seurata säännöllisesti, jotta vanhan teknologian poistuessa markkinoilta, valinta seuraavan teknologian suhteen pystytään tekemään nopeammin ja paremmin.

Asiakkaiden toiveita tarjottavan IPS-palvelun suhteen tulee tarkkailla, ja palvelua voidaan kehittää niiden mukaan. Käytössä oleva IPS-teknologia ei välttämättä mahdollista kaikkien asiakkaiden toiveiden täyttämistä, ja toiveet on syytä pitää mielessä seuraavaa teknologiaa valitessa.

Käyttöön valitun IPS-teknologian Ciscon tuki päättyy 26. huhtikuuta 2018 [48]. Tähän päivämäärään mennessä täytyy siis selvittää seuraava teknologia, jolla tuotteen tarjoamista jatketaan siitä eteenpäin.

# 6. YHTEENVETO

Asiakasjärjestelmien suojaamisen kannalta IPS-järjestelmässä korostuvat suorituskyvyllisten ja tarkkuuteen vaikuttavien seikkojen lisäksi toiminnan raportointiin ja kustomointiin liittyvät ominaisuudet.Lähtökohtana käytettävän teknologian ja sitä käyttävän laitteiston valintaan tulee olla omat tarpeet ja lopputuotteeseen suunnitellut ominaisuudet. IPS-järjestelmän suorituskyky vaikuttaa suoraan siihen, miten suurelle asiakasmäärälle sillä voidaan tarjota palvelua. Järjestelmän korkea tarkkuus taas mahdollistaa mahdollisimman vähäisen päivittäisen ylläpidon. Ylläpidon tarvetta laskee myös toiminnan mahdollisimman kattava ja helppo automatisoitavuus. Erilaiset ja helposti muokattavat raportointimahdollisuudet auttavat niin ylläpitäjiä kuin asiakastakin seuraamaan järjestelmän toimintaa.

Tuotteistuksen kannalta on myös tärkeä huomioida IPS:stä aiheutuva kulurakenne. Käytännössä tuote kannattaa rakentaa jonkin olemassa olevan IPS-teknologian päälle, jolloin hankinta- ja lisensointi kuluja vastaan saadaan aikaan merkittäviä säästöjä järjestelmän ylläpidosta. Ylläpitokustannukset kannattaa minimoida, koska ne tulevat kuitenkin olemaan todennäköisesti merkittävin kuluerä luotavan IPS-tuotteen elinkaaren aikana.

Tämän työn puitteissa suunniteltiin ja luotiin Ciscon IPS-teknologiaan perustuva IPS-suodatusta tarjoava palvelu. Vastaavanlainen palvelu olisi ollut mahdollista toteuttaa myös jollakin toisella IPS-teknologialla, mutta kyseinen Ciscon ratkaisu vastasi tällä kertaa parhaiten siihen kohdistuneisiin vaatimuksiin. Sekään ei kuitenkaan ole täysin ongelmaton. Kaikkia ominaisuuksia, joita tuotteeseen haluttiin, ei pystytty suoraan Ciscon teknologialla toteuttamaan. Osa ominaisuuksista on mahdollista rakentaa myöhemmin, mutta ne vaativat IPS:stä saatavan datan käsittelyä ulkopuolisissa järjestelmissä.

Luodun IPS-tuotteen elinkaari tulee todennäköisesti jatkumaan pidemmälle kuin sen toteutukseen valitun IPS-teknologian elinkaari. Uuden teknologian valinta onkin hyvä mahdollisuus kehittää nyt luotua tuotetta eteenpäin ja tuoda siihen uusia ominaisuuksia. Tämän työn pohjalta pystytään paremmin laatimaan kriteerejä myös tähän elinkaaren vaiheeseen, jotta tuote pystyy tulevaisuudessa palvelemaan sekä sen tarjoajan että asiakkaiden tarpeita paremmin.

Kaiken kaikkiaan tämä työ saavutti sille asetetut tavoitteet. Olemassa olevista IPS-teknologioista valittiin tilanteeseen sopivin vaihtoehto, ja sen toiminnallisuus tuotteistettiin asiakkaille tarjottavan IPS-palvelun muodossa.

# LÄHTEET


[1] Symantec. Internet Security Threat Report, 2015. Saatavissa (viitattu 12.3.2016): https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[2] Critical Infrastructure Readiness Report, 2015. Saatavissa (viitattu 24.3.2016): http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

[3] Ping of Death Attack, 2006. Saatavissa (viitattu 24.3.2016): https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=2154

[4] PCI-DSS v3.1, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, April 2015, s. 115.

[5] Mukhopadhyay, I., Chakraborty, M., Chakrabarti, S., A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems, Journal of Information Security, Vol 2, 2011, s. 28-38.

[6] Kemmerer, R., Vigna, G., Intrusion Detection: A Brief History and Overview, 2002. Saatavissa (viitattu 12.3.2016): http://www.computer.org/csdl/mags/co/2002/04/r4s27.pdf

[7] Gartner. Defining the Next-Generation Firewall, 2009 Saatavissa (viitattu 12.3.2016): http://img1.custompublish.com/getfile.php/1434855.1861.sqqycbrdwq/Defining+the+Next-Generation+Firewall.pdf

[8] Scarfone, K., Mell, P., Guide to Intrusion Detection and Prevention Systems (IDPS), 2007, NIST Special Publication 800-94. Saatavissa (viitattu 12.3.2016):http://ecinetworks.com/wp-content/uploads/bsk-files-manager/86_SP800-94.pdf

[9] Kurose, J., Ross, K., Computer Networking, Pearson Education, USA, 2008, s.878.

[10] Cisco. Protecting Industrial Control Systems with Cisco IPS Industrial Signatures, 2015.Saatavissa (viitattu: 5.9.2015): http://www.cisco.com/c/en/us/about/security-center/protecting-industrial-control-systems-networks-ips.html

[11] Cisco. Using the Service Control Engine and Deep Packet Instepction in the Data Center, 2008. Saatavissa (viitattu: 16.4.2016):

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/SCE_DPI.html

[12] Rash, M., Orebaugh, A., Clark, G., Pinkard, B., Babbin, J., Intrusion Prevention and Active Response, Syngress, USA, 2005, s. 424.

[13] Liu, H., Li, Z. Methodology of Network Intrusion Detection System Penetration Testing. Proceedings of Web-Age Information Management, Zhangjiajie, China, 2008, s. 546-551.

[14] Yu, D., Frincke, D. Towards survivable intrusion detection system. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, January 2004, s. 299-308.

[15] Ghorbani, A., Lu, W., Tavallaee, M., Network intrusion detection and prevention: concepts and techniques, Vol 47, Springer Science & Business Media, 2009.

[16] Dickerson, J., Juslin, J., Koukousoula, O, Fuzzy intrusion detection, Proceedings of IFSA World Congress and 20th North American Fuzzy Information Processing Society, July, 2001, pp. 1506–1510.

[17] Ho, C. Y., Lai, Y. C., Chen, I. W., Wang, F. Y., Tai, W. H. Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems, IEEE Communications Magazine, March 2012, pp. 146-154.

[18] Ensighten. Just One Second Delay In Page-Load Can Cause 7% Loss In Customer Conversions. Saatavissa (viitattu:28.3.2016): https://info.ensighten.com/rs/ensighten/images/just-one-second-delay-in-page-load-can-cause-7-percent-loss-in-customer-conversions.pdf

[19] Schaelicke, L., Slabach, T., Moore, B., & Freeland, C., Characterizing the performance of network intrusion detection sensors, Proceedings of Recent Advances in Intrusion Detection, 6th International Symposium, Pittsburgh, PA, USA, September 8-10, 2003, Lecture Notes in Computer Science, Volume 2820, s. 155-172.

[20] Cisco. Cisco Services for Intrusion Prevention Systems Customer Q&A, 2009. Saatavissa (viitattu: 12.3.2016): http://www.cisco.com/en/US/services/ps2827/ps6076/services_qa0900aecd8022e962.pdf

[21] Dokas, P., Ertoz, L., Kumar, V., Lazarevic, A., Srivastava, J., Tan, P., Data mining for network intrusion detection, Proceedings of NSF Workshop on Next Generation Data Mining, Baltimore,USA, 2002.

[22] Lee, W., Cabrera, J., Thomas, A., Balwalli, N., Saluja, S., Zhang, Y.Performance adaptation in real-time intrusion detection systems. Proceedings of Recent Advances in Intrusion Detection, 5th International Symposium, Zurich, Switzerland, 2002.

[23] Lee, W., Fan, W., Miller, M., Stolfo, S., Zadok, E. Toward cost-sensitive modeling for intrusion detection and response, Journal of Computer Security, vol 10, 2002, s. 5-22.

[24] Elisa. Tietoturva, 2015. Saatavissa (viitattu 6.9.2015): https://kauppa.saunalahti.fi/#!/palvelut/tietoturva

[25] Elisa. Kilpeä palvelunestohyökkäyksiä vastaan, 2014. Saatavissa (viitattu 6.9.2015): http://hub.elisa.fi/kilpea-palvelunestohyokkayksia-vastaan/

[26] Elisa. Elisa Palomuuripalvelu, 2015. Saatavissa (viitattu 6.9.2015): https://oma.elisa.fi/yrityksille/info/tuotteet-ja-palvelut/tuotteet/elisa-palomuuripalvelu/

[27] Sonera. Sonera Verkkosuoja, 2015. Saatavissa (viitattu 6.9.2015): http://www.sonera.fi/yrityksille/tuotteet+ja+palvelut/tietoliikennepalvelut/verkon+ja+paatelaitteiden+tietoturva/sonera+verkkosuoja?intcmp=b2b-soneraverkkosuoja-tuoteryhmasivu-palvelunosto

[28] Sonera. Sonera Palomuuri, 2015. Saatavissa (viitattu 6.9.2015): http://www.sonera.fi/yrityksille/tuotteet+ja+palvelut/tietoliikennepalvelut/verkon+ja+paatelaitteiden+tietoturva/sonera+palomuuri?intcmp=b2b-sonerapalomuuri-tuoteryhmasivu-palvelunosto

[29] Akamai. Kona Site Defender, 2014. Saatavissa (viitattu 6.9.2015): https://www.akamai.com/us/en/multimedia/documents/product-brief/kona-site-defender-product-brief.pdf

[30] Cloudflare. Plans, 2015. Saatavissa (viitattu 6.9.2015): https://www.cloudflare.com/plans

[31] Akamai. Client reputation, 2015. Saatavissa (viitattu 6.9.2015): https://www.akamai.com/us/en/solutions/products/cloud-security/client-reputation.jsp

[32] Imperva. Complete Website Security and Performance, 2015. Saatavissa (viitattu 6.9.2015): https://www.incapsula.com/

[33] Ulkoasiainministeriö. Katakri – tietoturvallisuuden auditointityökalu viranomaisille, 2015. Saatavissa (viitattu 6.9.2015): http://formin.finland.fi/public/download.aspx?ID=142173&GUID={7DF3B93D-6E25-4269-8A12-655D7FABEED6}

[34] Cisco. Cisco Firepower Next-Generation Firewall Data Sheet, 2016. Saatavilla (viitattu 12.4.2016): http://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-736661.html

[35] Cisco. Cisco ASA IPS Module Quick Start Guide, 2012. Saatavilla (viitattu: 3.4.2016): http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/ips/ips_qsg.html

[36] Cisco. Intrusion Prevention for the Cisco ASA 5500-X Series, 2013. Saatavilla (viitattu: 23.11.2015): http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-x-series-next-generation-firewalls/data_sheet_c78_459036.pdf

[37] Cisco. Cisco Services for IPS, 2015. Saatavilla (viitattu 23.11.2015): http://tools.cisco.com/security/center/ipshome.x?i=62

[38] Cisco. Cisco Intrusion Prevention System Signatures Frequently Asked Questions, 2015. Saatavilla (viitattu 23.11.2015): http://www.cisco.com/web/about/security/intelligence/ips_sig_faq.html

[39] Cisco. Risk Rating and Threat Rating: Simplify IPS Policy Management, 2015. Saatavilla (viitattu 11.5.2016): http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-series-sensors/prod_white_paper0900aecd806e7299.html

[40] Cisco. Integrating Cisco Security Agent with Cisco Intrusion Prevention System, 2015. Saatavilla (viitattu 11.5.2016):http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-series-sensors/prod_white_paper0900aecd805c389a.html

[41] Cisco. Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.0, 2014. Saatavilla (viitattu: 18.4.2016): http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_collaboration.html

[42] Halleen, G., Kellogg, G., Security Monitoring with Cisco Security MARS, Pearson Education, USA, 2007, s.336.

[43] Cisco. Cisco Intrusio Prevention System CLI Configuration Guide for IPS 7.1, 2013. Saatavilla (viitattu: 12.3.2016): http://www.cisco.com/c/en/us/td/docs/security/ips/7-1/configuration/guide/cli/cliguide71.pdf

[44] Zuech, R., Khoshgoftaar, T., Seliya, N., Njafabadi, M., Kemp, C., A New Intrusion Detection Benchmarking System, Proceedings of the Twenty-Eighth International Florida Artificial Intelligence Research Society Conference, Hollywood, USA, 2015.

[45] Tenable Network Security. Nessus Professional, 2016. Saatavissa (viitattu 3.4.2016): https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/DS_NessusProfessional_v6.5.pdf

[46] Acunetix. Audit Your Website Security with Acunetix Web Vulnerability Scanner, 2016. Saatavissa (viitattu: 16.4.2016): http://www.acunetix.com/vulnerability-scanner/

[47] Wordpress.org. Releases Category Archive, 2016. Saatavissa (viitattu: 16.4.2016): https://wordpress.org/news/category/releases/

[48] Cisco. End-of-Sale for Cisco Services for Intrusion Prevention System Support Program, 2014. Saatavissa (viitattu: 16.4.2016): http://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/eos-ips-support-program.pdf

# LIITE A: LUOTU TUNNISTE

```
signatures 60000 0
sig-description
sig-name AMBTT-132
sig-string-info AMBTT-132
no sig-comment
sig-creation-date 20151112
sig-type Vulnerability
exit
engine service-http
event-action produce-alert|deny-packet-inline
regex
specify-uri-regex yes
uri-regex \/[P|p][O|o][R|r][T|t][A|a][L|l]\/[L|l][O|o][G|g][I|i][N|n]
exit
specify-arg-name-regex yes
arg-name-regex [L|l][A|a][N|n][G|g][I|i][D|d]
specify-arg-value-regex yes
arg-value-regex .*--\>
exit
exit
exit
service-ports 80
exit
event-counter
event-count-key AxBx
exit
alert-frequency
summary-mode summarize
summary-interval 120
summary-key AxBx
exit
exit
specify-mars-category yes
mars-category Info/Misc|Penetrate/ClientExploit/Web
exit
exit
```

# LIITE B: ACUNETIX-SKANNAUKSEN TULOKSET ILMAN IPS:ÄÄ

## Scan of http://80.81.181.15:80/

### Scan details

| Scan information | |
|---|---|
| Start time | 4.4.2016 12:10:47 |
| Finish time | 4.4.2016 12:26:35 |
| Scan time | 15 minutes, 48 seconds |
| Profile | IPS-testing |
| **Server information** | |
| Responsive | True |
| Server banner | Apache/2.2.15 (Red Hat) |
| Server OS | Unix |
| Server technologies | PHP |

### Threat level

acunetix threat level

Level 3: High

**Acunetix Threat Level 3**

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution

| | |
|---|---|
| **Total alerts found** | **30** |
| High | 20 |
| Medium | 3 |
| Low | 6 |
| Informational | 1 |

### Knowledge base

**WordPress web application**

WordPress web application version 3.0 was detected in directory /.

**WordPress users**

List of WordPress users for /:

- admin

**WordPress plugins**

List of plugins installed for WordPress /:

akismet version 2.3.0 (latest 3.1.10)
Akismet checks your comments against the Akismet Web service to see if they look like spam or not.

# LIITE C: ACUNETIX-SKANNAUKSEN TULOKSET IPS:N KANSSA

## Scan of http://80.81.181.15:80/

### Scan details

| Scan information | |
|---|---|
| Start time | 4.4.2016 16:24:11 |
| Finish time | 4.4.2016 16:34:18 |
| Scan time | 10 minutes, 7 seconds |
| Profile | IPS-testing |
| **Server information** | |
| Responsive | True |
| Server banner | Apache/2.2.15 (Red Hat) |
| Server OS | Unix |
| Server technologies | PHP |

### Threat level


**Acunetix Threat Level 3**

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution


### Knowledge base

**WordPress web application**

WordPress web application version 3.0 was detected in directory /.

**WordPress users**

List of WordPress users for /:

- admin

**WordPress plugins**

List of plugins installed for WordPress /:

akismet version 2.3.0 (latest 3.1.10)
Akismet checks your comments against the Akismet Web service to see if they look like spam or not.